ZyXEL X-550

XtremeMIMO™ 802.11g Wireless Broadband Router

User's Guide

February 2006
Version 1.1

Copyright

Copyright ©2006 by ZyXEL Communications Corporation

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patents' rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement[1]

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Certifications

Go to www.us.zyxel.com

- Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- Select the certification you wish to view from this page.

[1] Refer to the *Quick Start Guide* for model specific FCC statement.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two (2) years from the date of purchase. During the warranty period and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

NOTE

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization (RMA) number. Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Online Registration

Register online at http://us.zyxel.com/ for free future product updates and information.

Customer Support

When contacting your Customer Support Representative, please have the following information ready:

- Serial number for your specific product
- Warranty information
- Date you received or purchased your product
- Brief description of the problem including any steps that you have taken before contacting the ZyXEL Customer Support Representative

	SUPPORT E-MAIL	TELEPHONE[2]	WEB SITE	REGULAR MAIL
NORTH AMERICA	support@zyxel.com	+1-800-978-7222	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.

[2] "+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

XtremeMIMO™ 802.11g Wireless Broadband Router ..... **i**

Copyright ..... **ii**

Federal Communications Commission (FCC) Interference Statement ..... **iii**

ZyXEL Limited Warranty ..... **iv**

Customer Support ..... **v**

Table of Contents ..... **vi**

Preface ..... **viii**

Chapter 1 Getting To Know Your X-550 ..... **1-2**

1.1 About Your ZyXEL X-550 ..... *1-2*

1.2 Features *1-2*

1.3 Hardware Overview *1-3*

1.3.1 Real Panel 1-3

1.3.2 Front Panel LEDs 1-4

1.4 Installation Considerations *1-5*

1.5 Getting Started *1-5*

Chapter 2 Wireless LAN Networking **2-1**

2.1 Overview *2-1*

2.2 SSID *2-1*

2.3 Channel *2-1*

2.4 Transmission Rate (Transfer Rate) *2-1*

2.5 Wireless Network Application *2-1*

Chapter 3 Using the Configuration Menu **3-1**

3.1 BASIC *3-2*

3.1.1 Setup Wizards 3-2

3.1.2 BASIC - WAN 3-3

3.1.3 BASIC - LAN 3-6

3.1.4 BASIC - DHCP 3-7

3.1.5 BASIC - Wireless 3-9

3.2 ADVANCED *3-13*

3.2.1 ADVANCED - Game Hosting 3-13

3.2.2 ADVANCED - Virtual Server 3-15

3.2.3 ADVANCED - Applications 3-17

3.2.4 ADVANCED - StreamEngine™ 3-19

3.2.5 ADVANCED - Routing 3-21

3.2.6 ADVANCED - Access Control 3-22

3.2.7 ADVANCED - WEB Filter 3-24

3.2.8 ADVANCED - MAC Filter 3-25

3.2.9 ADVANCED - Firewall 3-26
3.2.10 ADVANCED - Inbound Filter 3-27
3.2.11 ADVANCED - Wireless 3-29
3.2.12 ADVANCED - Schedules 3-30
3.3 TOOLS 3-32
3.3.1 TOOLS - Admin 3-32
3.3.2 TOOLS - Time 3-34
3.3.3 TOOLS - Syslog 3-35
3.3.4 TOOLS - Email 3-36
3.3.5 TOOLS - System 3-37
3.3.6 TOOLS - Firmware 3-38
3.3.7 Tools - DDNS (Dynamic DNS) 3-39
3.4 STAUS 3-41
3.4.1 STATUS - Device info 3-41
3.4.2 STATUS - Wireless 3-41
3.4.3 STATUS - Logs 3-42
3.4.4 STATUS - Statistics 3-44

Glossary i

Preface

Congratulations on your purchase of the **XtremeMIMO**™ X-550 Wireless Broadband Router. This manual is designed to guide you through the configuration of your ZyXEL X-550 for its various applications.

This manual may refer to the X-550 or 802.11g Secure Wireless Broadband Router with Firewall as the Router.

Note: Register your product online to receive e-mail notices of firmware upgrades and information at www.us.zyxel.com

About This User's Manual

This User's Guide is designed to guide you through the configuration of your X-550 using the web configurator(GUI). The web configurator parts of this guide contain background information on features configurable by web configurator.

Related Documentation

- Refer to the included CD for support documents.
- Quick Start Guide
- The Quick Start Guide is designed to help you get up and running right away. They contain connection information and instructions on getting started.
- Refer to the product page at www.us.zyxel.com for information on product certifications.
- ZyXEL Glossary and Web Site
- Please refer to www.us.zyxel.com for an online glossary of networking terms and additional support documentation.

User's Guide Feedback

Help us help you. E-mail all User's Guide-related comments, questions or suggestions for improvement to support@zyxel.com. Thank you.

Syntax Conventions

- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to use one of the predefined choices.
- The choices of a menu item are in **Bold Arial** font.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels and then Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels and then click Modem**.
- For brevity's sake, we will use "e.g." as a shorthand for "for instance" and "i.e." for "that is" or "in other words" throughout this manual.
- The following conventions are used in this manual:

THE NOTE SYMBOL INDICATES ADDITIONAL INFORMATION ON THE TOPIC AT HAND.

THE TIP SYMBOL INDICATES HELPFULL INFORMATION AND TIPS TO IMPROVE YOUR NETWORK EXPERIENCE.

THE CAUTION SYMBOL ALERTS YOU TO SITUATIONS THAT MAY DEGRADE YOUR NETWORKING EXPERIENCE OR COMPROMISE YOUR SECURITY.

LIKE NOTES AND TIPS, THE IMPORTANT SYMBOL INDICATES INFORMATION THAT CAN IMPROVE NETWORKING. THIS INFORMATION SHOULD NOT BE OVERLOOKED.

Package Contents

- X-550 XtremeMIMOTM Wireless Broadband Router
- CAT-5 Ethernet Cable (All the X-550's Ethernet ports are Auto-MDIX)
- Power Adapter (5.0V, 2A)
- Support CD

Using a power supply with a different voltage than the one included with your product will cause damage and void the warranty for this product.

Minimum System Requirements

- Ethernet-Based Cable or DSL Modem
- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter and CD-ROM Drive
- Internet Explorer Version 6.0 or Netscape Navigator Version 7.0 and Above.

Chapter 1
Getting To Know Your X-550

This chapter introduces the ZyXEL X-550 and prepares you to use the ZyXEL Utility.

1.1 About Your ZyXEL X-550

The ZyXEL X-550 **XtremeMIMO**™ Wireless Broadband Router is an 802.11g high-performance, wireless router that supports high-speed wireless networking in Home, SOHO, or even SMB environments.

Unlike most routers, the X-550 provides data transfers at up to 108 Mbps (compared to the standard 54 Mbps) when coupled with other MIMO products. The X-550 is also backwards compatible with older 802.11b networks making it a true versatile device. This means there is no need to change your entire network to maintain connectivity. 802.11b naturally has a lower throughput rate than 802.11g, but you will not lose the ability to communicate when you incorporate the 802.11g standard into your 802.11b network. You may choose to slowly change your network by gradually replacing the 802.11b devices with 802.11g devices.

1.2 Features

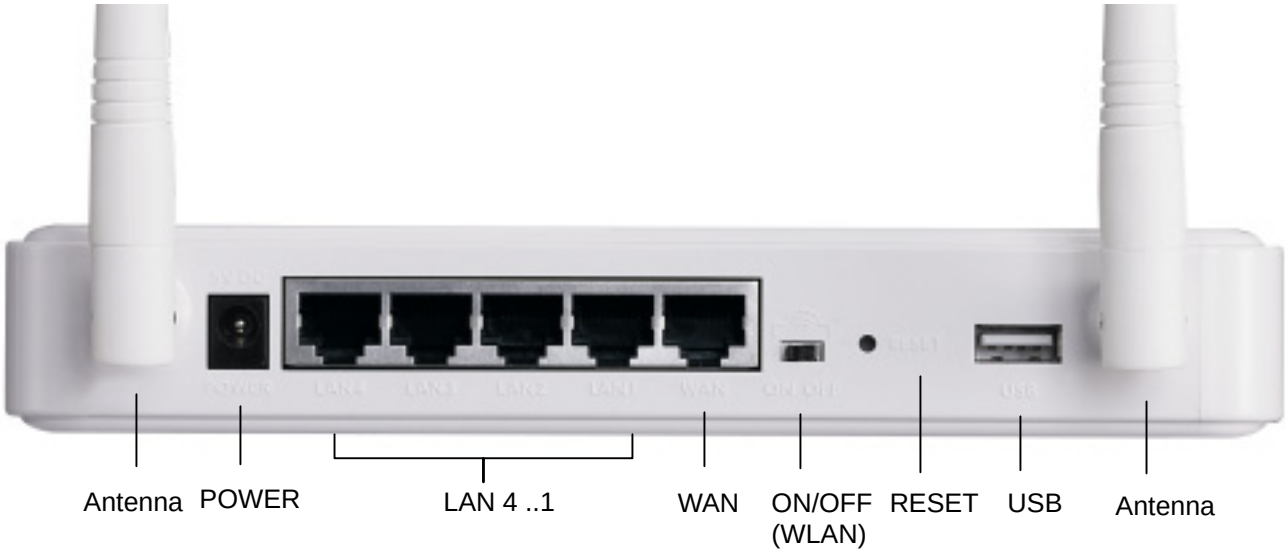
- Supports IEEE 802.11b/g 2.4GHz WLAN with 2.412 to 2.484GHz frequency band operation
- Provides MIMO advantages
- Intelligent receiving with directional antennas enable faster throughput and longer ranges
- Intelligent transmissions enable a more efficient performing network
- Built-in StreamEngine™ feature allows intelligent and automatic traffic prioritizing
- Data rates of 1,2.5.5,6,9, 11,12,18,24,36,48,54Mbps and Turbo Mode speeds up to 108Mbps.

Turbo Mode is an Atheros™ proprietary speed boosting technology that must be used in conjunction with other devices using the Atheros™ radio technology

- Hardware encryption for Wi-Fi Protected Access (WPA2/WPA) and Wired Equivalent Privacy (WEP) without performance degradation
- WPA2/WPA (Wi-Fi Protected Access) authorizes and identifies users based with a secret key that changes automatically at a regular interval, for example:
  Pre Shared Key mode means that the home user, without a RADIUS server,
  will obtain a new security key every time he or she connects to the network, vastly improving the safety of communications on the said network
- User-friendly configuration and diagnostic utilities
- Connect multiple computers to a Cable or DSL modem to share a single Internet connection
- DHCP server enables all networked computers to automatically receive IP addresses
- Web-based interface for easy management and configuration
- Supports special applications that require multiple connections
- Equipped with four 10/100 Ethernet ports, one WAN port all with Auto MDI/MDIX

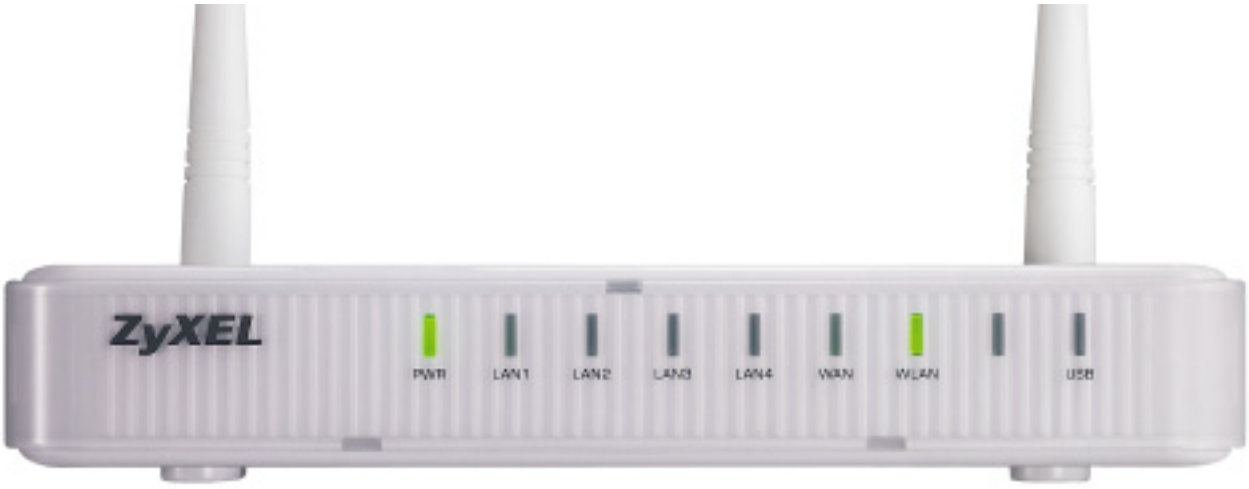
1.3 Hardware Overview

1.3.1 Real Panel



Connections and/or Features	Description
POWER	Connect the barrel type connector of the included *power adaptor to this power socket. CAUTION **Please use only the included power adapter to power the X-550.**
LAN 1-4 **Auto MDI/MDIX LAN Ports**	These ports automatically sense the cable type when connecting to Ethernet-enabled computers.
WAN **Auto MDI/MDIX WAN Port**	The Internet connection from your Cable or DSL model is attached to this port.
ON/OFF **WLAN Slide Switch**	Use this switch to turn off the Wireless side of the X-550 without going into the configuration menus.
RESET **Reset Button**	The Reset button is used to restore the X-550 back to the factory default settings. Push for 10 seconds to reset to factor defaults.
USB **USB Port**	The USB port is used for Microsoft®'s Windows Connect Now feature
Antenna	The ZyXEL X-550 includes 2 fixed external Smart Antennas and 2 internal Smart Antennas.

1.3.2 Front Panel LEDs



LED's	Description
PWR **POWER**	A solid light indicates a proper connection to the power supply.
LAN **LAN1~4**	A solid light indicates a connection to an Ethernet-enabled computer. Blinking indicates data transmission.
WAN	A solid light indicates a connection to a Cable or DSL broadband modem. Blinking indicates data transmission.
WLAN	A solid light indicates that the wireless connection is ready. Blinking indicates data transmission.
USB	The USB LED will flash 3 times indicating that your X-550 has successfully connected using the Microsoft® Windows Connect Now feature. IMPORTANT **Please keep note of this LED when using Microsoft® Windows Connect Now**

1.4 Installation Considerations

The following recommendations should only be used as a reference. Your optimal solution may vary.

The X-550 XtremeMIMO Wireless Router allows you to access your network using a wireless connection, from virtually anywhere within its operating range. Keep in mind; however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit said range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home, home office or business. Follow these basic guidelines to maximize your range in your environment:

- Keep the number of walls and ceilings between the X-550 and other network devices to a minimum - each wall or ceiling can reduce your wireless product's range significantly. Position your devices so that the number of walls or ceilings is minimized.
- Be aware of the direct line between network devices. A wall, 1.5 feet thick (.5 meters), at a 45-degree angle will appear to be almost 3 feet (1 meter) thick due to the angle of incidence. Position devices so the signal will travel perpendicular through a wall or ceiling (instead of at an angle) for better reception.
- Building Materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.
- Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate extreme RF noise such as microwaves or wireless *telephones.
  Note: depends on operating frequency

1.5 Getting Started

For a wireless setup at home, please check to make sure you have the following:

- You will need broadband Internet access (a Cable or DSL line into your home or office)
- Consult with your Cable or DSL provider for proper installation of the modem.
- Connect the Cable or DSL modem to the X-550 Wireless Broadband Router (WAN port).

Chapter 2
Wireless LAN Networking

This chapter provides background information on general wireless LAN networking technology and terminology.

THE INFORMATION IN THIS SECTION IS FOR YOUR REFERENCE. CHANGING NETWORK SETTINGS AND PARTICULARLY SECURITY SETTTINGS SHOULD ONLY BE DONE BY AN AUTHORIZED ADMINISTRATOR.

2.1 Overview

This section introduces the wireless LAN(WLAN) and some basic scenarios.

2.2 SSID

The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

2.3 Channel

A radio frequency used by a wireless device is called a channel.

2.4 Transmission Rate (Transfer Rate)

The X-550 provides various transmission (data) rate options for you to select. Options available are: Best (Auto), 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 22 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps, and 108Mbps. In most networking scenarios, the factory default setting, Best (Auto) provides the most efficient and optimal performance. This setting allows your X-550 to operate at the maximum transmission (data) rate at any given time. When the communication quality drops below a certain level, the X-550 automatically switches to a lower transmission (data) rate. The X-550 will gradually increases the transmission (data) rate again when communication levels improve and will keep on doing so until reaching the highest available transmission (data) rate.

2.5 Wireless Network Application

Wireless LAN networking works in either of the two methodologies: ad-hoc and infrastructure. In infrastructure mode, wireless devices communicate to a wired LAN via access points. Each access point and its wireless devices are known as a Basic Service Set (BSS). An Extended Service Set (ESS) is two or more BSSs in the same subnet. In ad hoc mode (also known as peer-to-peer mode), wireless devices communicate with each other directly and do not use an access point. This is an Independent BSS (IBSS).

To connect to a wired network within a coverage area using access points, set the X-550 operation mode to Infrastructure (BSS). To set up an independent wireless workgroup without an access point, use Ad-hoc (IBSS) mode.

Ad-Hoc (IBSS)

Ad-hoc mode does not require an access point or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

Figure 2-1 IBSS Example

To set up an ad-hoc network, configure all wireless stations in ad-hoc network type and use the same SSID and channel.

Infrastructure (BSS)

When a number of wireless stations are connected using a single AP, you have a Basic Service Set (BSS).

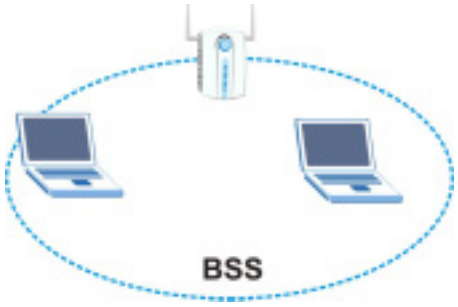


Figure 2-2 BSS Example

A series of overlapping BSS and a network medium, such as an Ethernet forms an Extended Service Set (ESS) or infrastructure network. All communication is done through the AP, which relays data packets to other wireless stations or devices connected to the wired network. Wireless stations can then access resource, such as the printer, on the wired network.

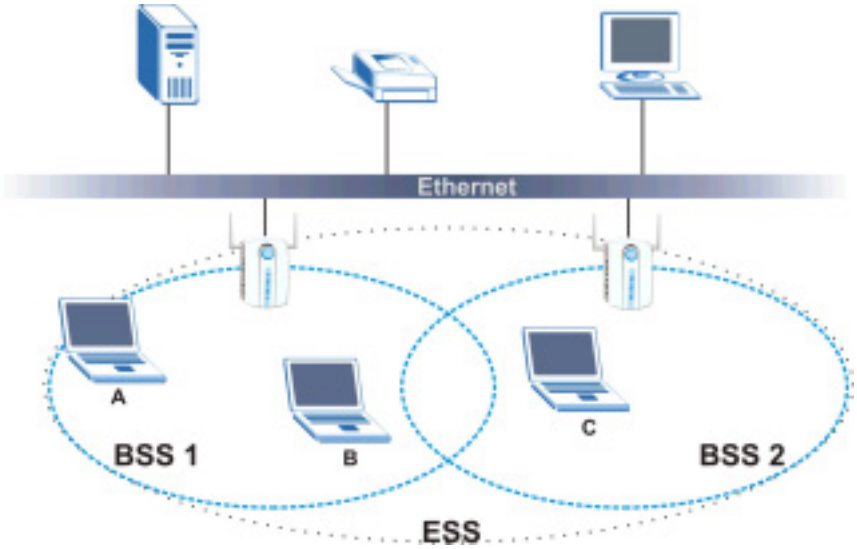


Figure 2-3 Infrastructure Network Example

Roaming

In an infrastructure network, wireless stations are able to switch from one BSS to another as they move between the coverage areas. During this period, the wireless stations maintain uninterrupted connection to the network. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate AP depending on the signal strength, network utilization or other factors.

The following figure depicts a roaming example. When wireless station **B** moves to position **X**, the ZyXEL X-550 in wireless station **B** automatically switches the channel to the one used by access point **2** in order to stay connected to the network.

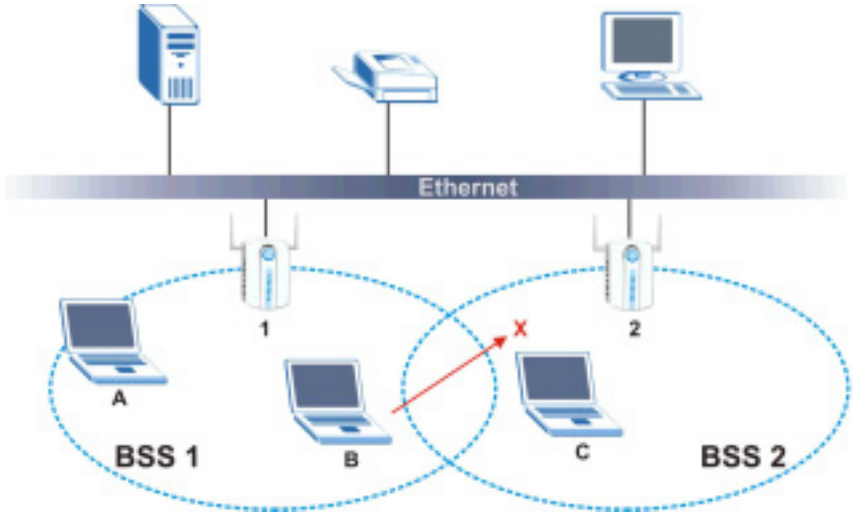


Figure 2-4 Roaming Example

Chapter 3
Using the Configuration Menu

This chapter describes how to configure your ZyXEL Router

Whenever you want to configure your X-550, you can access the Configuration Menu by opening the Web-browser and typing in the IP Address of the X-550. The X-550's default IP Address is http://192.168.10.1

- Open the Web browser.
- Type in the **IP Address** of the Router (http://192.168.10.1).

Figure 3-1 ADVANCED – Wireless

If you have changed the default IP Address assigned to the X-550, make sure to enter the correct IP Address.

- Select **admin** in the **User Name** field.
  if this is your first time configuring your X-550, the default user will already be admin
- Type in **1234** in the **Password** field.
  1234 is the factory default password
- Click **Login** to proceed into the Configuration Menu of the X-550

3.1 BASIC

The Basic tab provides the following configuration options:

- **Start** **brings you back to the Wizard and Introductions page*
- **WAN** **allows you to manually configure your WAN settings*
- **LAN** **allows you to manually configure your LAN settings*
- **DHCP** **allows you to manually input DHCP settings*
- **Wireless** **allows you to manually configure your WLAN settings*

3.1.1 Setup Wizards

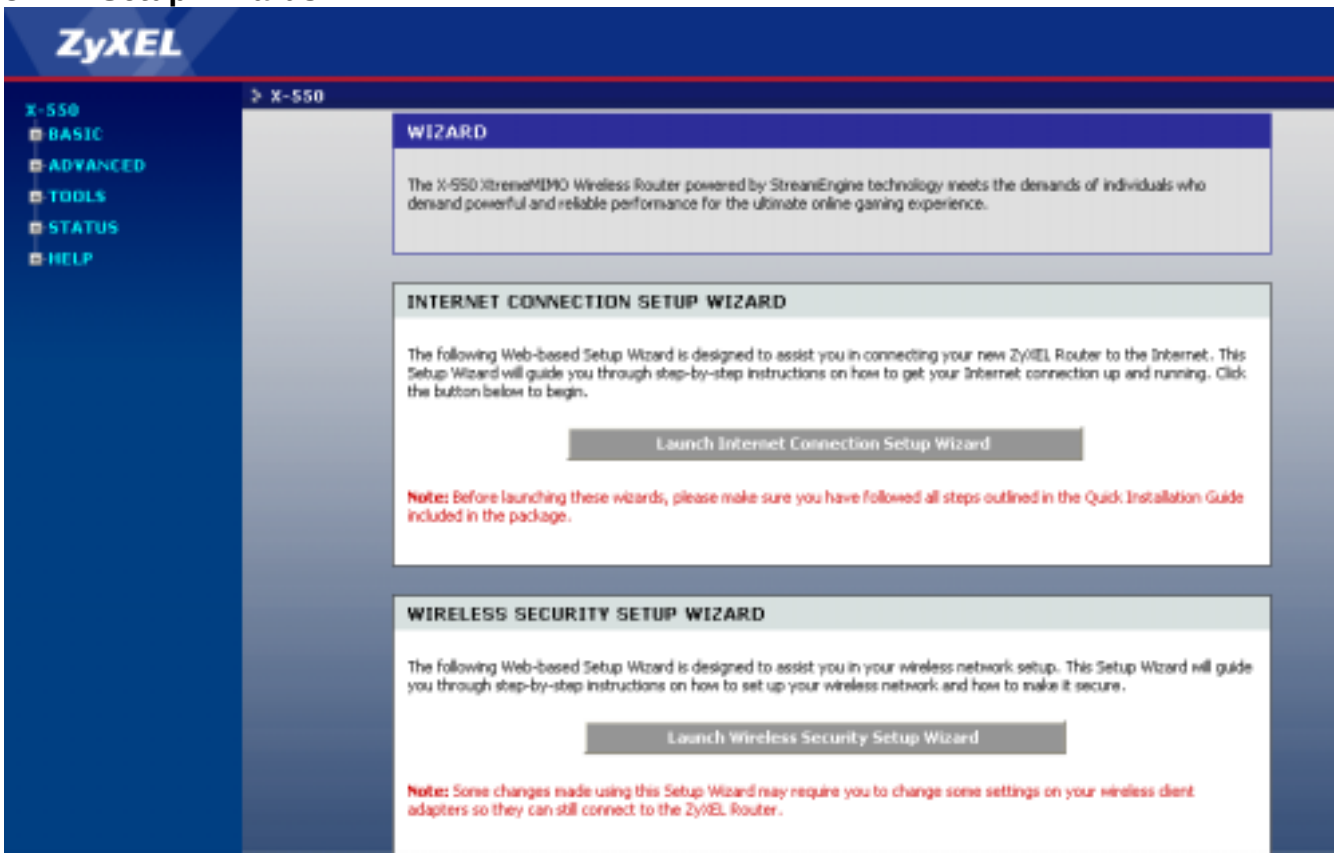

ZyXEL
X-550
BASIC
ADVANCED
TOOLS
STATUS
HELP
> X-550
WIZARD
The X-550 XtremeMIMO Wireless Router powered by StreamEngine technology meets the demands of individuals who demand powerful and reliable performance for the ultimate online gaming experience.
INTERNET CONNECTION SETUP WIZARD
The following Web-based Setup Wizard is designed to assist you in connecting your new ZyXEL Router to the Internet. This Setup Wizard will guide you through step-by-step instructions on how to get your Internet connection up and running. Click the button below to begin.
Launch Internet Connection Setup Wizard
Note: Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.
WIRELESS SECURITY SETUP WIZARD
The following Web-based Setup Wizard is designed to assist you in your wireless network setup. This Setup Wizard will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.
Launch Wireless Security Setup Wizard
Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the ZyXEL Router.

Figure 3-2 Setup Wizard

INTERNET CONECTION SETUP WIZARD

The on-board wizard guides you through the following basic router setup steps:

- **Set your Password**
- **Select your Time Zone**
- **Configure your Internet Connection**
- **Save your Settings and Connect to the Internet**

WIRELESS SECURITY SETUP WIZARD

This guides you through the steps for setting up wireless security in your wireless network:

- **Name your Wireless Network**
- **Set your Wireless Security Key**
- **Secure your Wireless Network**

3.1.2 BASIC - WAN

The WAN (Wide Area Network) section is where you configure how your internal network connects to the Internet. There are several connection types to choose from: Static IP, DHCP & PPPoE*. If you are unsure of your connection method, please contact your Internet Service Provider for details.

If using PPoE, any PPPoE client software on your computer must be removed or disabled prior to the setup of your X-550.

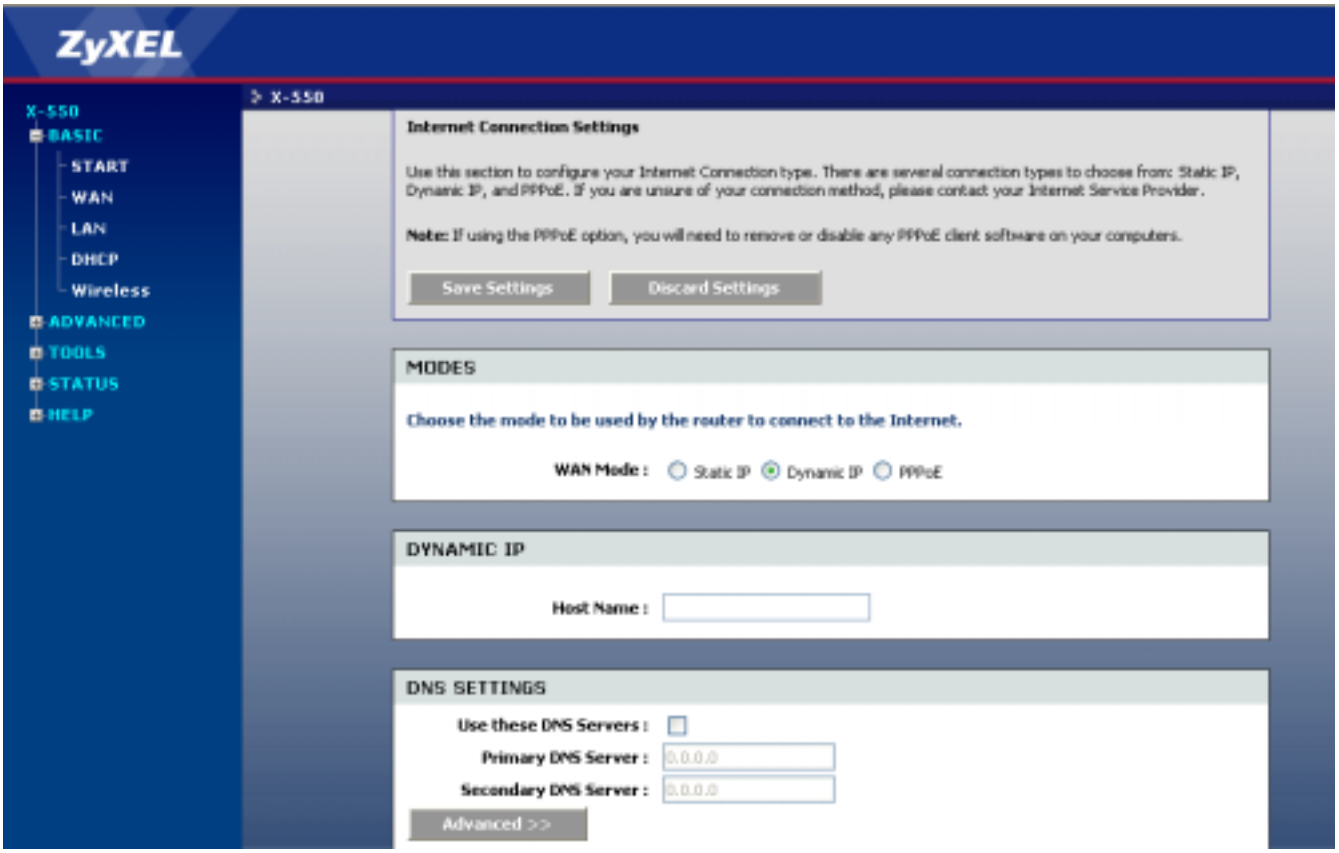

ZyXEL
X-550
BASIC
START
WAN
LAN
DHCP
Wireless
ADVANCED
TOOLS
STATUS
HELP
X-550
Internet Connection Settings
Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, Dynamic IP, and PPPoE. If you are unsure of your connection method, please contact your Internet Service Provider.
Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.
Save Settings
Discard Settings
MODES
Choose the mode to be used by the router to connect to the Internet.
WAN Mode : Static IP Dynamic IP PPPoE
DYNAMIC IP
Host Name :
DNS SETTINGS
Use these DNS Servers :
Primary DNS Server : 0.0.0.0
Secondary DNS Server : 0.0.0.0
Advanced >>

Figure 3-3 BASIC - WAN

STATIC IP WAN Mode

Use Static WAN Mode when your ISP provides you with an IP address that does not change. The IP information is manually entered in your IP configuration settings. You must enter the IP address, Subnet Mask, Gateway, Primary DNS Server, and Secondary DNS Server. Your ISP will provide you with all of this information.

DYNAMIC IP WAN Mode

Use Dynamic IP WAN Mode when your ISP assigns an IP address to you every time you connect onto the Internet. If you do not know, please contact your ISP for information to whether or not your connection is using Dynamic IP. Some ISP's require you to make some settings to your network before your router can be connected to the Internet.

Host Name: Certain ISP's require specific computer Host Names. The Host Name identifies your system to the ISP's server.

PPPoE WAN Mode

Select this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection. This method of connection requires you to enter a **Username** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

Service Name: Some ISP's may require that you enter a *Service Name.

Only enter a Service Name if your ISP requires one.

Reconnect Mode:

Typically PPPoE connections are not always on. The Wireless router allows you to set the reconnection mode. The settings are:

- **Always on:** A connection to the Internet is always maintained.
- **On demand:** A connection to the Internet is made when needed.
- **Manual:** Every time you wish to connect the internet, you MUST enter the configuration menu and click on the **Connect** button

***Maximum Idle Time:** Time the device will idle before the PPPoE connection is disconnected.

The Maximum Idle Time value is only used for the "On demand" connection mode.

Advanced

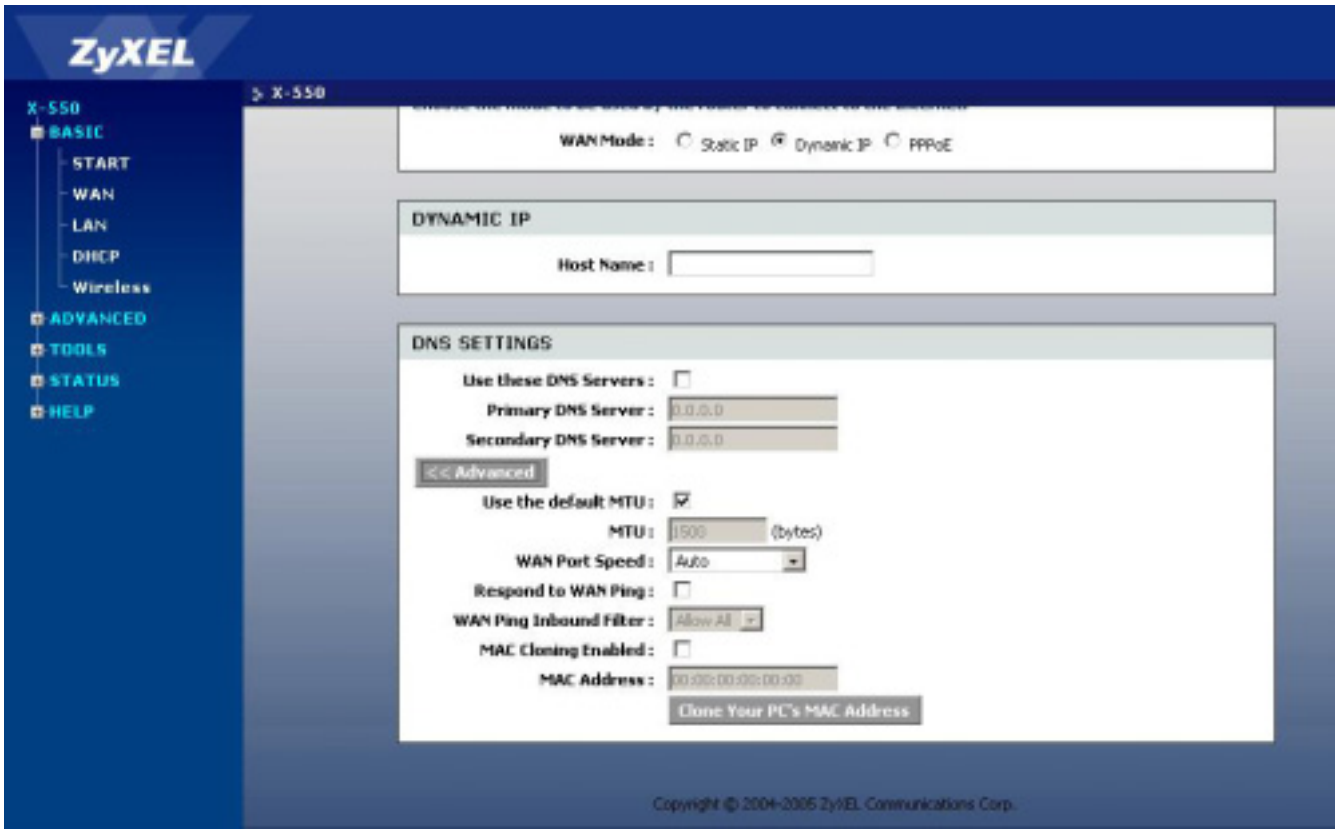


Figure 3-4 WAN- Advanced

Any changes to these options apply to all WAN modes *Static IP/Dynamic IP/PPPoE.

Use These DNS Servers:

This option should be enabled if your ISP requires you to enter the DNS Server information. You will then be able to enter a primary and secondary DNS server.

Use the default MTU:

If this option is checked (the default case), the router selects the usual MTU settings for the type of WAN interface in use. If this option is unchecked, the router uses the value of the MTU option (which follows).

MTU:

The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

WAN Port Speed:

Normally, this is set to "auto". If you have trouble connecting to the WAN, try the other settings.

Respond to WAN Ping:

If you leave this option unchecked, you are causing the public WAN IP address of the router not to respond to **ping** commands. Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.

WAN Ping Inbound Filter:

Select a filter that controls access as needed for WAN pings. If you do not see the filter you need in the list

of filters, go to the **ADVANCED -> Inbound Filter** screen and create a new filter.

MAC Cloning Enabled:

Some ISP's may check your computer's MAC address. Each networking device has its own unique MAC address defined by the hardware manufacturer. Some ISP's record the MAC address of the network adapter in the computer or router used to initially connect to their service. The ISP will then only grant Internet access to requests from a computer or router with this particular MAC address. Your new Wireless router has a different MAC address than the computer or router that initially connected to the ISP. To resolve this problem, the Wireless router has a special feature that allows you to clone (that is, replace the router's MAC address with) another MAC address.

MAC Address:

If you have enabled MAC Cloning, you can either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or copy the MAC address of a PC. To copy the MAC address of the computer that initially connected to the ISP, connect to the Wireless router using that computer and click the **Clone Your PC's MAC Address** button. The WAN port will then use the MAC address of the network adapter in your computer.

3.1.3 BASIC - LAN

These are the settings of the LAN (Local Area Network) interface for the router. The router's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface. It is recommended that you use the default settings if you do not have an existing network.

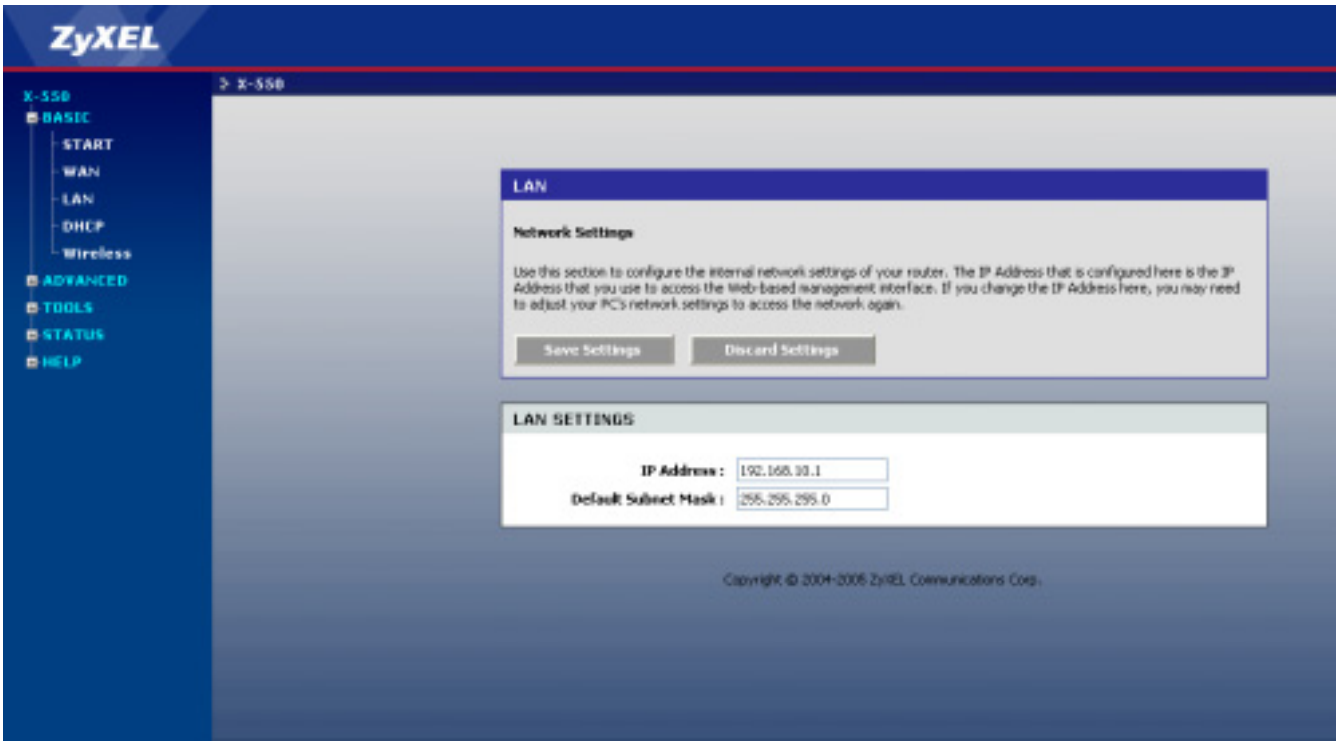


Figure 3-5 BASIC - LAN

IP Address: This is the IP address your router will be associated with on the local area network.

Default Subnet Mask: This is the subnet mask of your router on the local area network.

3.1.4 BASIC - DHCP

DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN).

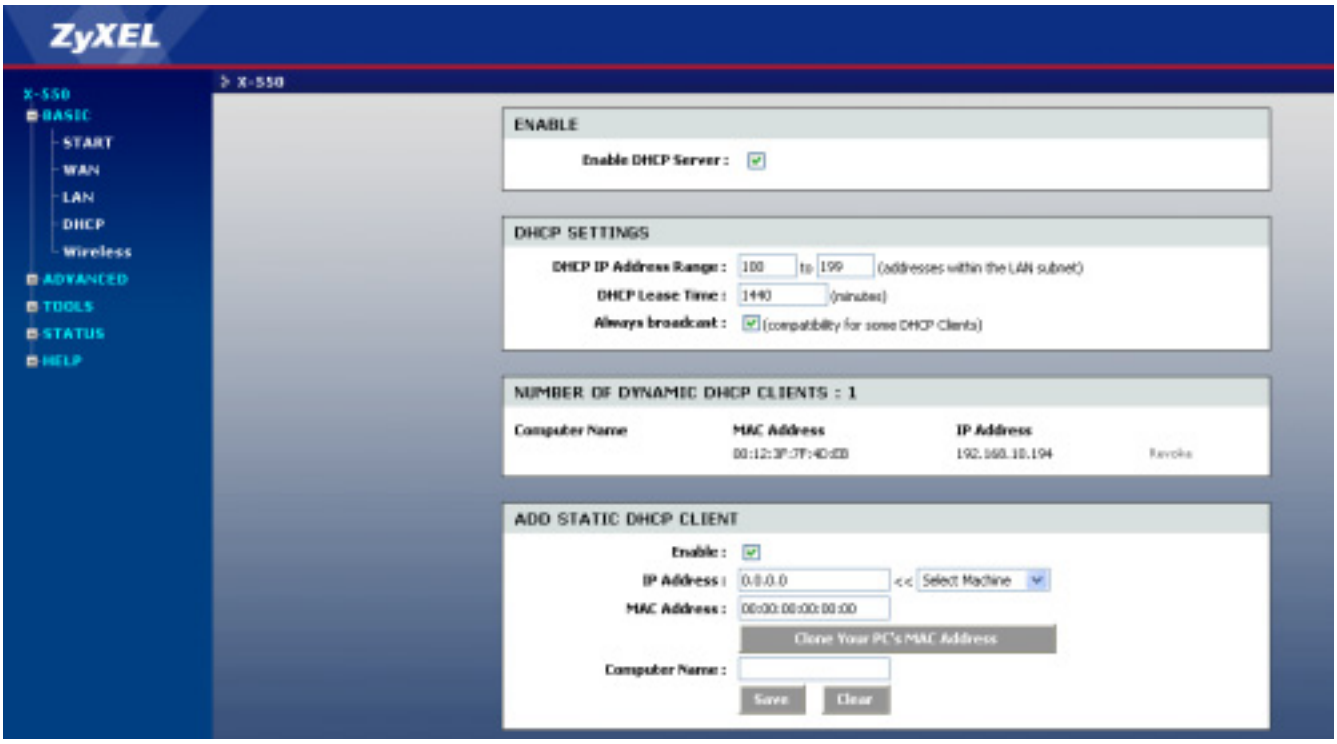


Figure 3-6 BASIC - DHCP

DHCP SETTINGS

Enable DHCP Server:

Once your Wireless router is properly configured and this option is enabled, the DHCP Server will manage the IP addresses and other network configuration information for computers and other devices connected to your Local Area Network. There is no need for you to do this yourself.

The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to "DHCP" or "Obtain an IP address automatically".

When you set **Enable DHCP Server**, the following options are displayed.

DHCP IP Address Range:

These two values (*from* and *to*) define a range of addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network. Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically.

It is possible for a computer or device that is manually configured to have an address that does reside within this range. In this case the address should be reserved (see **Static DHCP Client** below), so that the DHCP Server knows that this specific address can only be used by a specific computer or device.

Your Wireless router, by default, has a static IP address of 192.168.0.1. This means that addresses 192.168.0.2 to 192.168.0.254 (from 2 to 254) can be made available for allocation by the DHCP Server.

Example:
Your Wireless router uses 192.168.0.1 for the IP address. You've assigned a computer that you want to designate as a Web server with a static IP address of 192.168.0.3. You've assigned another computer that you want to designate as an FTP server with a static IP address of 192.168.0.4. Therefore the starting IP address for your DHCP IP address range needs to be 5 or greater.

Example:
Suppose you configure the DHCP Server to manage addresses From 100 To 199. This means that 3 to 99 and 200 to 254 are NOT managed by the DHCP Server. Computers or devices that use addresses from these ranges MUST be manually configured. Suppose you have a web server computer that has a manually configured address of 192.168.0.100. Because this falls within the "managed range" be sure to create a reservation for this address and match it to the relevant computer (see **Static DHCP Client** below).

DHCP Lease Time:

The amount of time that a computer may have an IP address before it is required to renew the lease. The initial lease designates the amount of time before the lease expires. If the client wishes to retain the address when the lease is expired then a new lease is established. If the lease expires and the address is no longer needed than another client may use the address.

Always Broadcast:

If all the computers on the LAN successfully obtain their IP addresses from the router's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the router's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the router to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.

NUMBER OF DYNAMIC DHCP CLIENTS

In this section you can see what LAN devices are currently leasing IP addresses.

Revoke:

The **Revoke** option is available for the situation in which the lease table becomes full or nearly full, you need to recover space in the table for new entries, and you know that some of the currently allocated leases are no longer needed. Clicking **Revoke** cancels the lease for a specific LAN device and frees an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network.

ADD/EDIT STATIC DHCP CLIENT

This option lets you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as if a device has a static IP address except that it must still request an IP address from the Wireless router. The Wireless router will provide the device the same IP address every time. Static DHCP is helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or use this option.

MAC Address:

To input the MAC address of your system, enter it in manually or connect to the Wireless router's Web-Management interface from the system and click the **Clone Your PC's MAC Address** button.

A MAC address is usually located on a sticker on the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33. If your network device is a computer and the network card is already located inside the computer, you can connect to the Wireless router from the computer and click the **Clone Your PC's MAC Address** button to enter the MAC address.

As an alternative, you can locate a MAC address in a specific operating system by following the steps below:

Windows 2000 Windows XP	Go to your Start menu, select Programs, select Accessories, and select Command Prompt. At the command prompt type **ipconfig /all** and hit Enter. The physical address displayed for the adapter connecting to the router is the MAC address.
Mac OS X	Go to the Apple Menu, select System Preferences, select Network, and select the Ethernet Adapter connecting to the Wireless router. Select the Ethernet button and the Ethernet ID will be listed. This is the same as the MAC address.

Computer Name:
You can assign a name for each computer that is given a static IP address. This may help you keep track of which computers are assigned this way.

Example: Game Server

STATIC DHCP CLIENT LIST

This shows clients that you have specified to have static DHCP address. An entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Static DHCP Client" section is activated for editing.

3.1.5 BASIC - Wireless

The wireless section is used to configure the wireless settings for your Wireless router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: **WEP, WPA-Personal, and WPA-Enterprise**. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires a RADIUS authentication server.

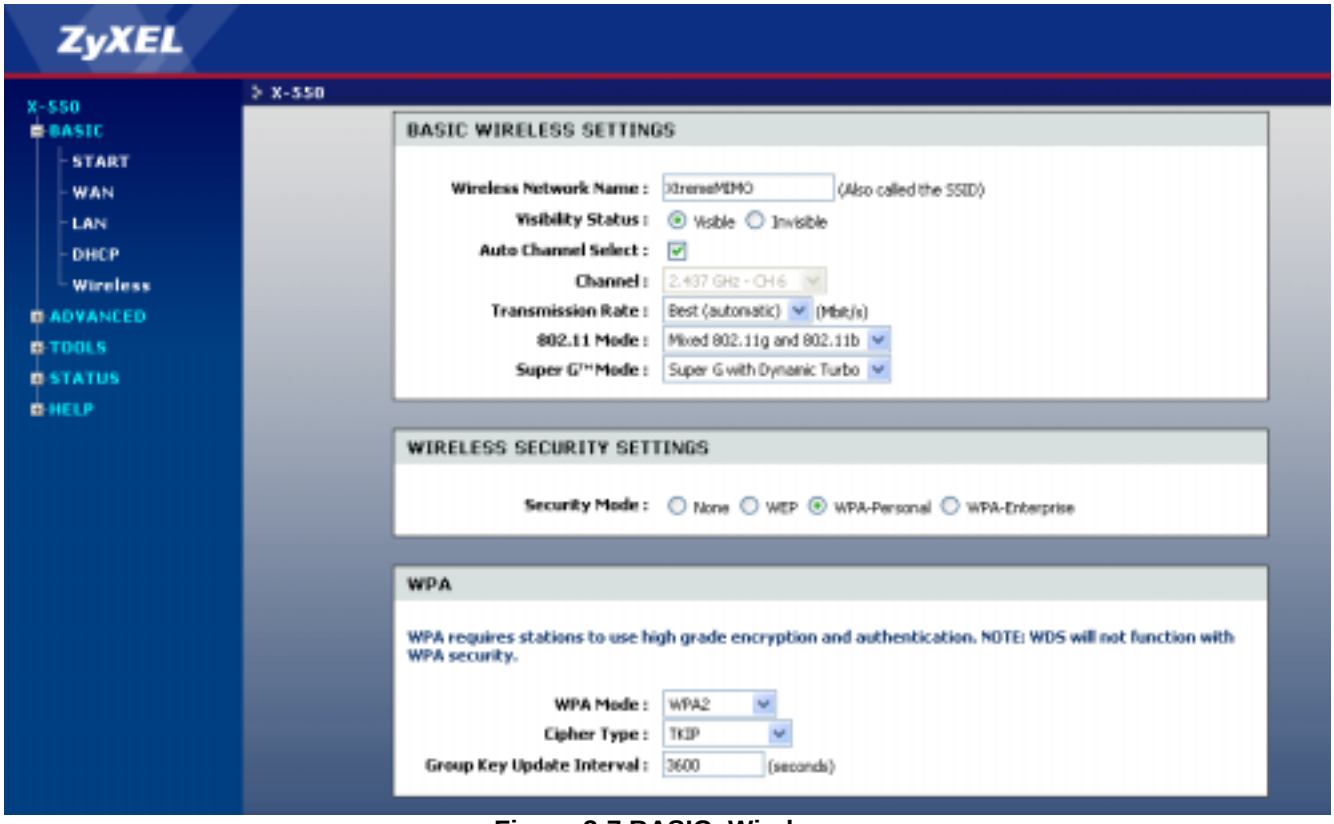


Figure 3-7 BASIC- Wireless

BASIC WIRELESS SETTING

Wireless Radio:

This indicates whether or not the WLAN of the X-550 is turned on or off. Please use the dip switch at the rear of the X-550 to manually enable or disable the WLAN.

Wireless Network Name:

When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is recommended to change from the factory default SSID.

Visibility Status:

The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

Auto Channel Select:

If you select this option, the router automatically finds the channel with least interference and uses that channel for wireless networking. If you disable this option, the router uses the channel that you specify with the following **Channel** option.

Channel:

A wireless network uses specific channels in the 2.4GHz wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

Transmission Rate:

By default the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.

802.11 Mode:

If all of your devices can connect in 802.11g Mode, you can change the mode to 802.11g only. If you have some devices that are 802.11b, leave the setting at Mixed.

Super G™ Mode:

Super G Turbo Modes must use channel 6 for communication. For Super G with Static Turbo, **802.11 Mode** must be set to 802.11g. For proper operation, RTS threshold and Fragmentation Threshold on the **ADVANCED -> Advanced Wireless** screen should both be set to their default values.

Super G Turbo mode must be used with Atheros™ wireless chipset. Please consult your client device manufacturer for more information.

Super G without Turbo:

Performance enhancing features such as Packet Bursting, FastFrames, and Compression.

Super G with Static Turbo:

This mode is not backwards compatible with non-Turbo (legacy) devices. This mode should only be enabled when all devices on the wireless network are Static Turbo enabled.

Super G with Dynamic Turbo:

This mode is backwards compatible with non-Turbo (legacy) devices. This mode should be enabled when some devices on the wireless network are not Turbo enabled but support other Super G features mentioned above.

WIRELESS SECUIRITY SETTING

WEP:

A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must

know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

Example:
64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.)

128-bit hexadecimal keys are exactly 26 characters in length. (456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption.)

64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.)

128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.)

WPA-Personal and WPA-Enterprise:

Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The **WPA Mode** further refines the variant that the router should employ.

WPA

WPA Mode:

WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the router associates only with clients that also support WPA2 security.

Cipher Type:

The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the "TKIP and AES" option, the router negotiates the cipher type with the client, and uses AES when available.

Group Key Update Interval:

The amount of time before the group key used for broadcast and multicast data is changed.

WPA-Personal

This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

PRE-SHARED KEY

The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Example: Wireless Networking technology enables ubiquitous communication

WPA-Enterprise

This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

EAP (802.1X)

Authentication Timeout: Amount of time before a client will be required to re-authenticate.

RADIUS Server IP Address: The IP address of the authentication server.

RADIUS Server Port: The port number used to connect to the authentication server.

RADIUS Server Shared Secret: A pass-phrase that must match with the authentication server.

MAC Address Authentication: If this is selected, the user must connect from the same computer whenever logging into the wireless network.

Advanced:

Optional Backup RADIUS Server:

This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the primary RADIUS server. The second RADIUS server is consulted only when the primary server is not available or not responding. The fields **Second RADIUS Server IP Address**, **RADIUS Server Port**, **Second RADIUS server Shared Secret**, **Second MAC Address Authentication** provide the corresponding parameters for the second RADIUS Server.

3.2 ADVANCED

The Advanced tab provides the following configuration options: **Game Hosting, Virtual Server, Applications, StreamEngine™, Routing, Access Control, Web Filter, MAC Filter, Firewall, Inbound Filter, Wireless and Schedules**.

3.2.1 ADVANCED - Game Hosting

Multiple connections are required by some applications, such as internet games, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). The Gaming section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats:

Range (50-100)
Individual (80, 68, 888)
Mixed (1020-5000, 689)

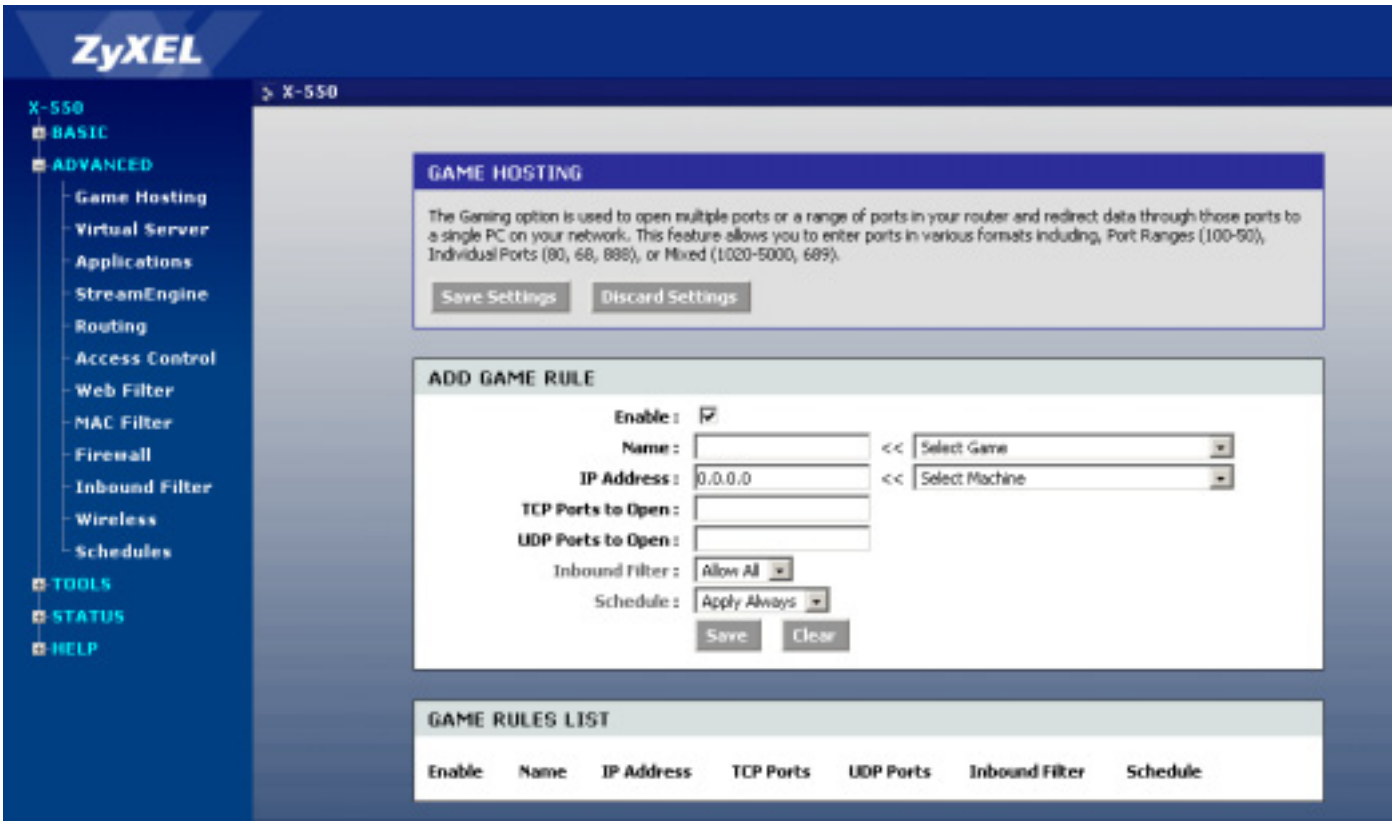


Figure 3-8 ADVANCED- Game Hosting

ADD GAME RULE

Here you can add entries to the Game Rules List below, or edit existing entries.

Example:

You are hosting an online game server that is running on a PC with a Private IP Address of 192.168.0.50. This game requires that you open multiple ports (6159-6180, 99) on the router so Internet users can connect.

Enable:

Each entry in Game Rules List can be active (enabled) or inactive (disabled)

Name:
Give the Gaming Rule a name that is meaningful to you, for example **Game Server**. You can also select from a list of popular games, and many of the remaining configuration values will be filled in accordingly. However, you should check whether the port values have changed since this list was created, and you must fill in the IP address field.

IP Address:
Enter the local network IP address of the system hosting the game server, for example **192.168.0.50**.

TCP Ports To Open:
Enter the TCP ports to open. [6159-6180, 99]

UDP Ports To Open:
Enter the UDP ports to open. [6159-6180, 99]

Inbound Filter:
Select a filter that controls access as needed for this game rule. If you do not see the filter you need in the list of filters, go to the **ADVANCED -> Web Filter** screen and create a new filter.

Schedule:
Select a schedule for the times when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the **TOOLS -> Schedules** screen and create a new schedule.

Save:
Clicking **Save** saves the new or edited Game Rule in the following list. After you are done applying all the Game Rules you wish to set, please click **Save Settings** to make the changes permanent on the X-550.

With this Gaming Rule enabled, all TCP and UDP traffic on ports 6159 through 6180 and port 99 is passed through the router and redirected to the Internal Private IP Address of your Game Server at 192.168.0.50.

GAME RULES LIST
The section shows the currently defined game rules. A game rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Game Rule" section is activated for editing.

3.2.2 ADVANCED - Virtual Server

The Virtual Server option gives Internet users access to services on your LAN. This feature is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a public port on your router for redirection to an internal LAN IP Address and LAN port.

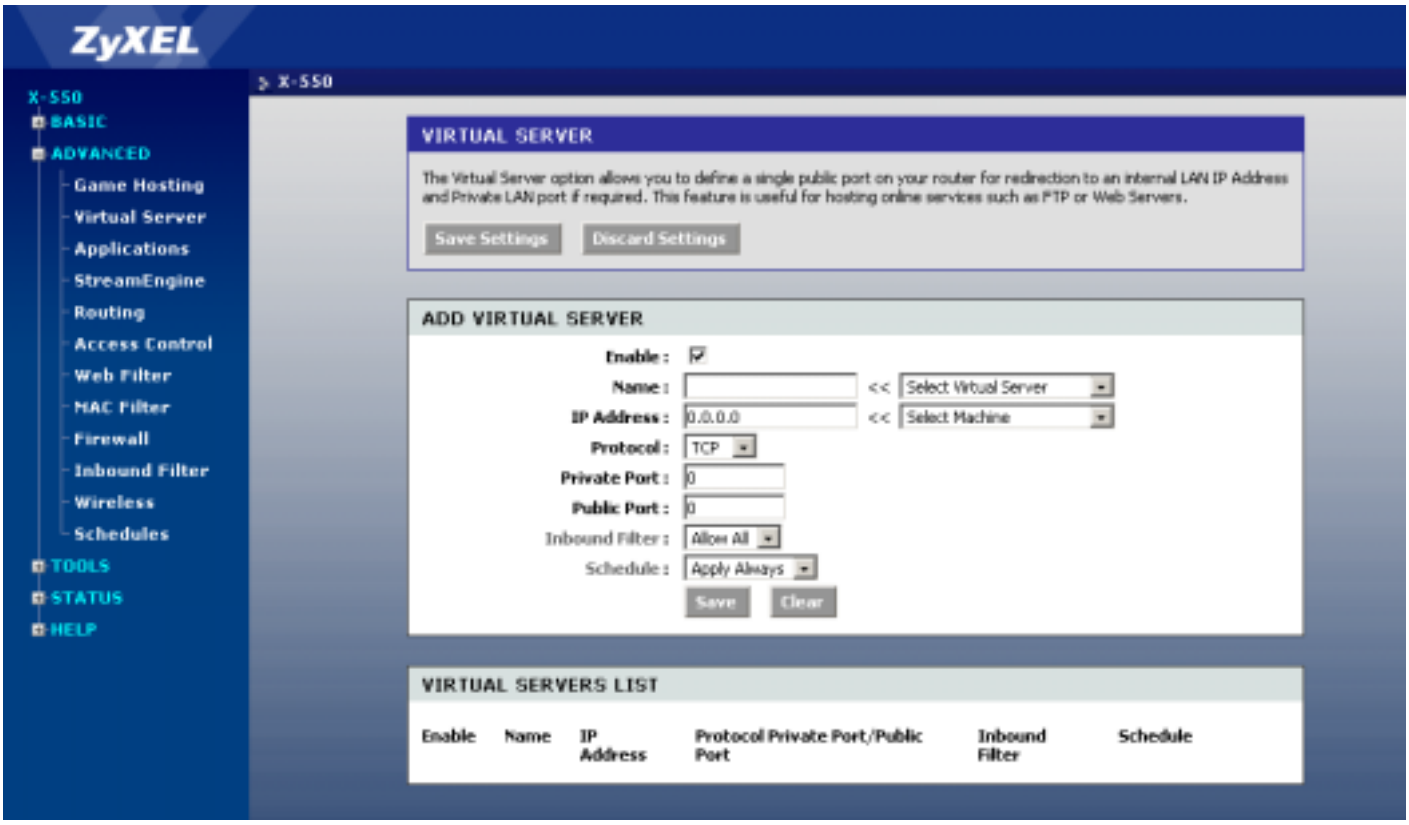


Figure 3-9 ADVANCED - Virtual Server

Example:

You are hosting a Web Server on a PC that has LAN IP Address of 192.168.0.50 and your ISP is blocking Port 80.

1. **Name** the Virtual Server (for example: **Web Server**)
2. Enter the **IP Address** of the machine on your LAN (for example: **192.168.0.50**)
3. Enter the **Private Port** as [80]
4. Enter the **Public Port** as [8888]
5. Select the **Protocol** - TCP
6. Ensure the schedule is set to **Always**
7. Click **Save** to add the settings to the Virtual Servers List
8. Repeat these steps for each Virtual Server Rule you wish to add. After the list is complete, click **Save Settings** at the top of the page.

With this Virtual Server entry, all Internet traffic on Port 8888 will be redirected to your internal web server on port 80 at IP Address 192.168.0.50.

ADD/EDIT VIRTUAL SERVER

In this section you can add an entry to the Virtual Servers List below or edit an existing entry.

Enable:
Entries in the list can be either active (enabled) or inactive (disabled).

Name:
Assign a meaningful name to the virtual server, for example **Web Server**. Several well-known types of virtual server are available from the "Select Virtual Server" list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.

IP Address:
The IP address of the system on your internal network that will provide the virtual service, for example **192.168.0.50**.

Protocol:
Select the protocol used by the service.

Private Port:
The port that will be used on your internal network.

Public Port:
The port that will be accessed from the Internet.

Inbound Filter:
Select a filter that controls access as needed for this virtual server. If you do not see the filter you need in the list of filters, go to the **ADVANCED -> Inbound Filter** screen and create a new filter.

Schedule:
Select a schedule for when the service will be enabled. If you do not see the schedule you need in the list of schedules, go to the **TOOLS -> Schedules** screen and create a new schedule.

Save:
Clicking **Save** saves the new or edited virtual server entry in the following list. When finished updating the virtual server entries, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

VIRTUAL SERVERS LIST

The section shows the currently defined virtual servers. A Virtual Server can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Virtual Server" section is activated for editing.

You might have trouble accessing a virtual server using its public identity (WAN-side IP-address of the gateway or its dynamic DNS name) from a machine on the LAN. Your requests may not be looped back or you may be redirected to the "Forbidden" page.

This will happen if you have an Access Control Rule configured for this LAN machine.

The requests from the LAN machine will not be looped back if Internet access is blocked at the time of access. To work around this problem, access the LAN machine using its LAN-side identity.

Requests may be redirected to the "Forbidden" page if web access for the LAN machine is restricted by an Access Control Rule. Add the WAN-side identity (WAN-side IP-address of the router or its dynamic DNS name) on the **ADVANCED -> Web Filter** screen to work around this problem.

3.2.3 ADVANCED - Applications

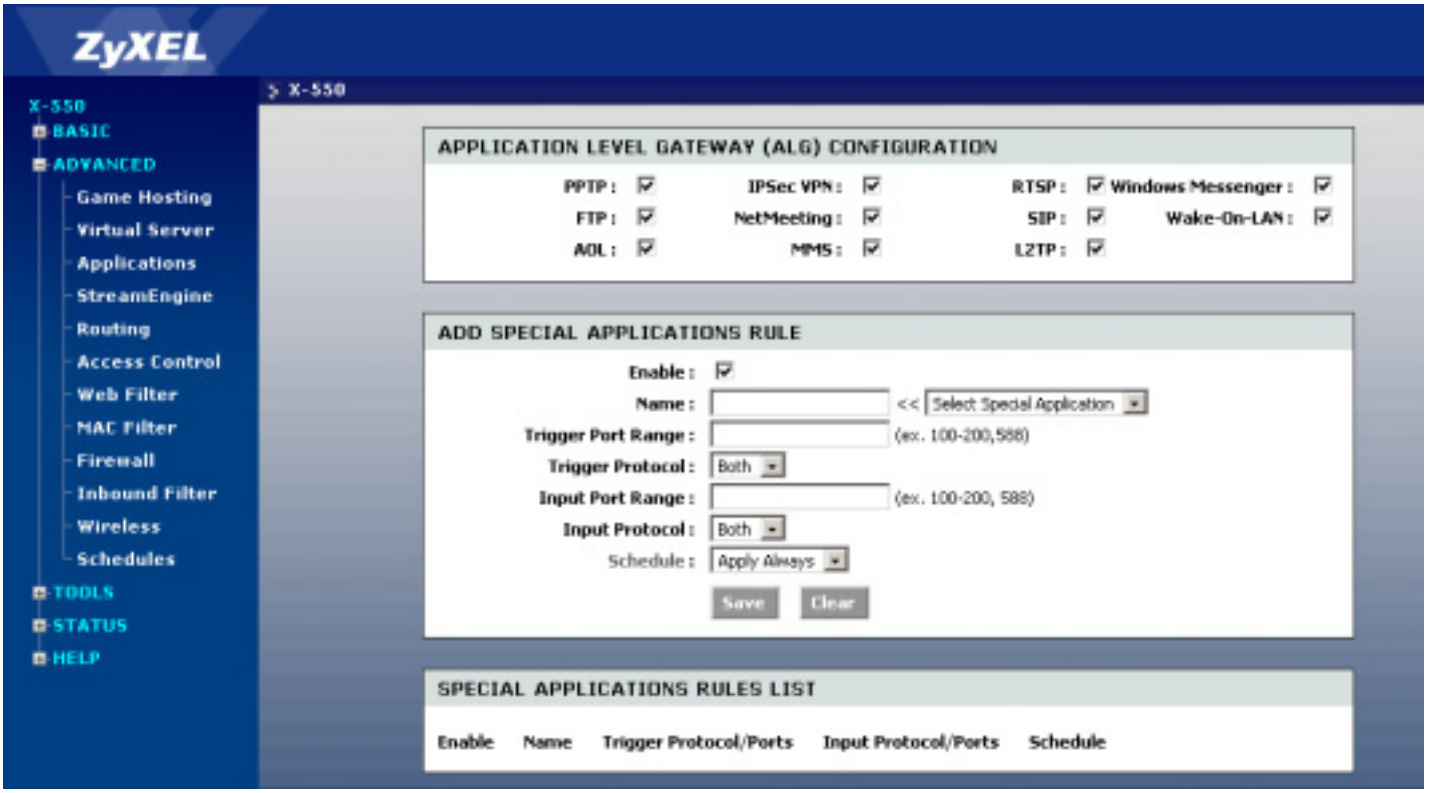


Figure 3-10 ADVANCED - Applications

APPLICATION LEVEL GATEWAY (ALG) CONFIGURATON

Here you can enable or disable ALGs. Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.

PPTP:

Enabling this feature allows multiple machines on the LAN to connect to their corporate network using the PPTP protocol.

IPSec VPN:

This feature allows multiple VPN clients to connect to their corporate network using IPSec protocol. Some VPN clients support traversal of IPSec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off.

Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

RTSP:

Enabling RTSP allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.

Windows Messenger:

Enabling this feature supports the use of Microsoft Windows Messenger (the Internet messaging client that ships with Microsoft Windows) on LAN computers. The SIP ALG must also be enabled when the Windows Messenger ALG is enabled.

FTP:

Enabling this feature allows FTP clients and servers to transfer data across NAT. Refer to the

ADVANCED -> Virtual Server page if you want to host an FTP server.

NetMeeting:
Allows Microsoft NetMeeting clients to communicate across NAT. Note that if you want your buddies to call you, you should also set up a virtual server for NetMeeting. Refer to the **ADVANCED -> Virtual Server** page for information on how to set up a virtual server.

SIP:
Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

Wake-On-LAN:
This feature enables forwarding of "magic packets" (that is, specially formatted wake-up packets) from the WAN to a LAN computer or other device that is "Wake on LAN" (WOL) capable. The WOL device must be defined as such on the **ADVANCED ->Virtual Server** page. The LAN IP address for the virtual server is typically set to the broadcast address 192.168.0.255. The computer on the LAN whose MAC address is contained in the magic packet will be awakened.

AOL:
Use this feature if you are experiencing frequent disconnects from the AOL server due to inactivity.

MMS:
This feature allows Windows Media Player, using MMS protocol, to receive streaming media from the internet.

L2TP:
Enabling this feature allows multiple machines on the LAN to connect to their corporate network using the L2TP protocol.

ADD SPECIAL APPLICATIONS RULE

The Special Application section is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. Special Applications rules apply to all computers on your internal network.

Example:

You need to configure your router to allow a software application running on any computer on your network to connect to a web-based server or another user on the Internet.

Name:

Enter a name for the Special Application Rule, for example **Game App**, which will help you identify the rule in the future. You can also select from a list of common applications, and the remaining configuration values will be filled in accordingly.

Trigger Port Range:

Enter the outgoing port range used by your application. [6500-6700]

Trigger Protocol:

Select the outbound protocol used by your application. [Both]

Input Port Range:

Enter the port range that you want to open up to Internet traffic. [6000-6200]

Input Protocol:

Select the protocol used by the Internet traffic coming back into the router through the opened port range. [Both]

Schedule:
Select a schedule for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the **TOOLS -> Schedules** screen and create a new schedule.

Save:

Clicking **Save** saves the new or edited Special Applications Rule in the following list. When finished updating the Special Applications entries, you must still click the **Save Settings** button at the top of the page to make the changes permanent.

With this Special Application Rule enabled, the router will open up a range of ports from 6000-6200 for incoming traffic from the Internet, whenever any computer on the internal network opens up an application that sends data to the Internet using a port in the range of 6500-6700.

SPECIAL APPLICATIONS RULES LIST

The section shows the currently defined special applications rules. A special applications rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Special Applications Rule" section is activated for editing.

3.2.4 ADVANCED - StreamEngine™

The StreamEngine™ feature helps improve your network gaming performance by prioritizing applications. By default, the StreamEngine™ settings are disabled.

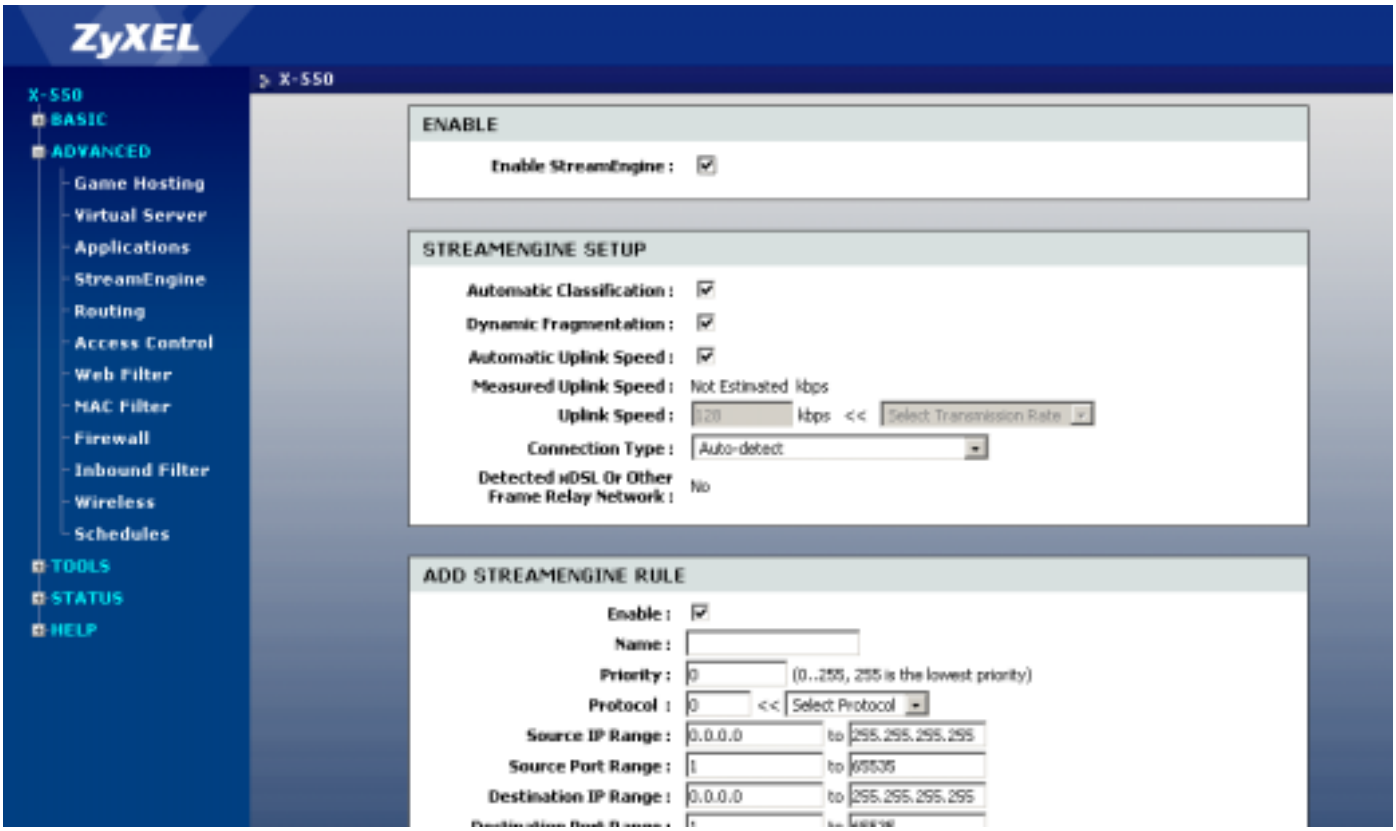


Figure 3-11 ADVANCED - StreamEngine

STREAMENGINE SETUP

Enable StreamEngine™:

This option is disabled by default. Enable it for better performance and experience with online games and other interactive applications, such as VoIP.

Automatic Classification:

This option is enabled by default so that your router will automatically determine which programs should

have network priority.

Dynamic Fragmentation:
This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones by breaking the large packets into several smaller packets.

Automatic Uplink Speed:
When enabled, this option causes the router to automatically measure the useful uplink bandwidth each time the WAN interface is re-established (after a reboot, for example).

Measured Uplink Speed:
This is the uplink speed measured when the WAN interface was last re-established. The value may be lower than that reported by your ISP as it does not include all of the network protocol overheads associated with your ISP's network. Typically, this figure will be between 87% and 91% of the stated uplink speed for xDSL connections and around 5 kbps lower for cable network connections.

Uplink Speed:
If Automatic Uplink Speed is disabled, this options allows you to set the uplink speed manually. Uplink speed is the speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISPs often specify speed as a downlink/uplink pair; for example, 1.5Mbits/284Kbits. For this example, you would enter "284". Alternatively you can test your uplink speed with a service such as www.dslreports.com. Note however that sites such as DSL Reports, because they do not consider as many network protocol overheads, will generally note speeds slightly lower than the Measured Uplink Speed or the ISP rated speed.

Connection Type:
By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as **Detected xDSL or Frame Relay Network**. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either "Static" or "DHCP" in the WAN settings, setting this option to **xDSL or Other Frame Relay Network** ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing **xDSL or Other Frame Relay Network** causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.

Detected xDSL or Frame Relay Network:
When **Connection Type** is set to **Auto-detect**, the automatically detected connection type is displayed here.

ADD STREAMENGINE RULE

Automatic classification will be adequate for most applications, and specific StreamEngine™ Rules will not be required. A StreamEngine™ Rule identifies a specific message flow and assigns a priority to that flow.

Enable:
Each entry in StreamEngine™ Rules List can be active (enabled) or inactive (disabled)

Name:
Create a name for the rule that is meaningful to you.

Priority:
The priority of the message flow is entered here. 0 receives the highest priority (most urgent) and 255 receives the lowest priority (least urgent).

Protocol:
The protocol used by the messages.

Source IP Range:
The rule applies to a flow of messages whose LAN-side IP address falls within the range set here.

Source Port Range:
The rule applies to a flow of messages whose LAN-side port number is within the range set here.

Destination IP Range:
The rule applies to a flow of messages whose WAN-side IP address falls within the range set here.

Destination Port Range:
The rule applies to a flow of messages whose WAN-side port number is within the range set here.

Save:
Clicking **Save** saves the new or edited StreamEngine™ Rule in the following list. When finished updating the StreamEngine™ rules, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

STREAMENGINE RULES LIST

The section shows the currently defined StreamEngine™ rules. A StreamEngine™ rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit StreamEngine™ Rule" section is activated for editing.

3.2.5 ADVANCED - Routing

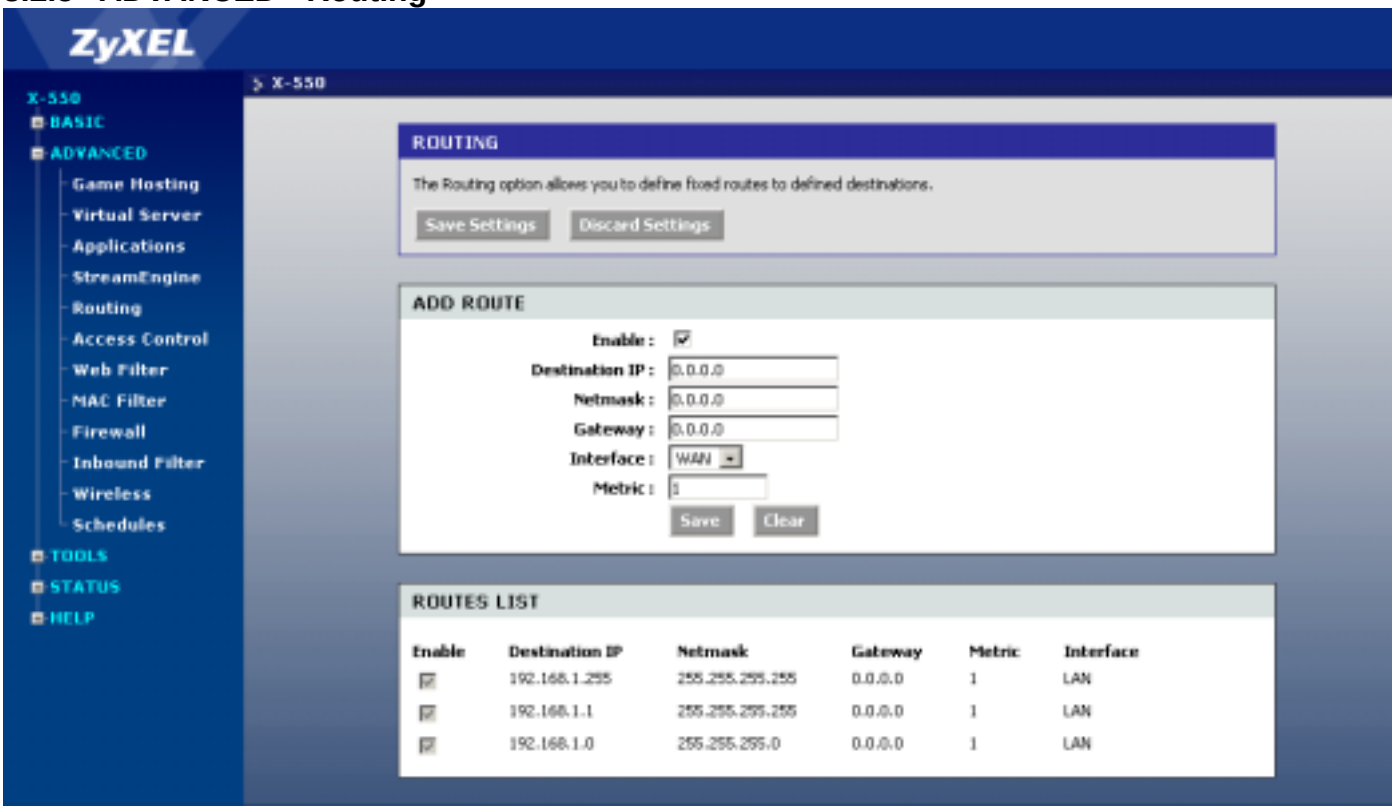


Figure 3-12 ADVANCED - Routing

ADD ROUTE

Adds a new route to the IP routing table or edits an existing route.

Enable:
Specifies whether the entry will be enabled or disabled.

Destination IP:
The IP address of packets that will take this route.

Netmask:
One bits in the mask specify which bits of the IP address must match.

Gateway:
Specifies the next hop to be taken if this route is used. A gateway of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified: LAN or WAN.

Interface:
Specifies the interface -- LAN or WAN -- that the IP packet must use to transit out of the router, when this route is used.

Metric:
The relative cost of using this route.

Save:
Clicking **Save** saves the new or edited route in the following list. When finished updating the routing table, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

ROUTES LIST

The section shows the current routing table entries. Certain required routes are predefined and cannot be changed. Routes that you add can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Route" section is activated for editing.

3.2.6 ADVANCED - Access Control

The Access Control section allows you to control access in and out of devices on your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications such as peer-to-peer utilities or games.

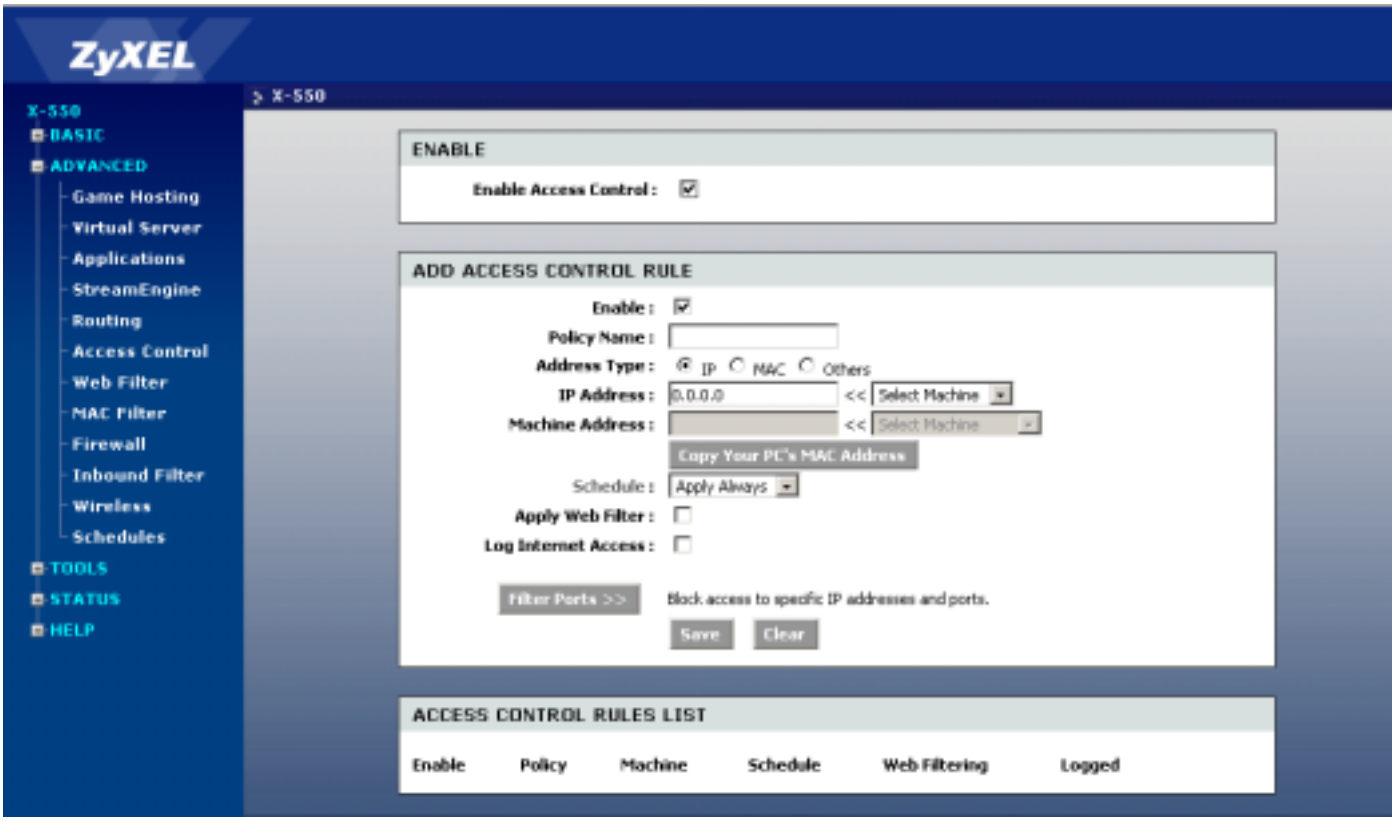


Figure 3-13 ADVANCED – Access Control

ENABLE

By default, the Access Control feature is disabled. If you need Access Control, check this option, and you will see the following configuration sections.

When Access Control is disabled, every device on the LAN has unrestricted access to the Internet. However, if you enable Access Control, Internet access is restricted for those devices that have an Access Control Rule configured for them. All other devices will have unrestricted access to the Internet.

ADD ACCESS CONTROL RULE

Access Control Rules specify what a LAN device is allowed to access. Here you can add entries to the **Access Control Rules** or edit existing entries.

Enable:

Each entry in Access Control Rules List can be active (enabled) or inactive (disabled)

Policy Name:

Create a name for this access control policy (rule) that is meaningful to you. Typically this would be a system name or user name; for example "Casey's PC".

Address Type:

Select the type of address on which you want to base the rule.

IP Address:

Enter the IP Address of the machine that you want the access control rule to apply to. Make sure that the device on the LAN either has a static IP address (that is, one that is not in the DHCP range) or is in the Static DHCP Client List (see **BASIC -> DHCP**).

Machine Address:

Enter the MAC Address of the machine that you want the access control rule to apply to. If you want to enter the MAC Address of the computer you are using, click the **Clone Your PC's MAC Address** button.

Others: If you want to restrict access for all devices that do not have an explicit rule configured for them, then select "Others" for the Address Type.

Schedule:

Select a schedule of the times when you want the policy to apply. If you do not see the schedule you need in the list of schedules, go to the **TOOLS -> Schedules** screen and create a new schedule.

Apply Web Filter:

With this option enabled, the specified system will only have access to the Web sites listed in the Web Filter section.

Log Internet Access:

If this option is enabled, all of the Web sites visited by the specified machine will be logged.

Filter Ports:

By clicking the **Filter Ports** button you can specify that the rule prohibit access to specific IP addresses and ports.

Save:

Clicking **Save** saves the new or edited access control rule in the following list. Repeat the process, creating an Access Control Rule for each of the devices on your LAN that needs access to the Internet. When finished updating the Access Control Rules, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

ACCESS CONTROL RULES LIST

This section shows the current access control rules. Rules can be changed by clicking the **Edit** icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "**Edit Access Control Rule**" section is activated for editing.

3.2.7 ADVANCED - WEB Filter

The **Web Filter** section is where you add the Web sites to be used for **Access Control**.

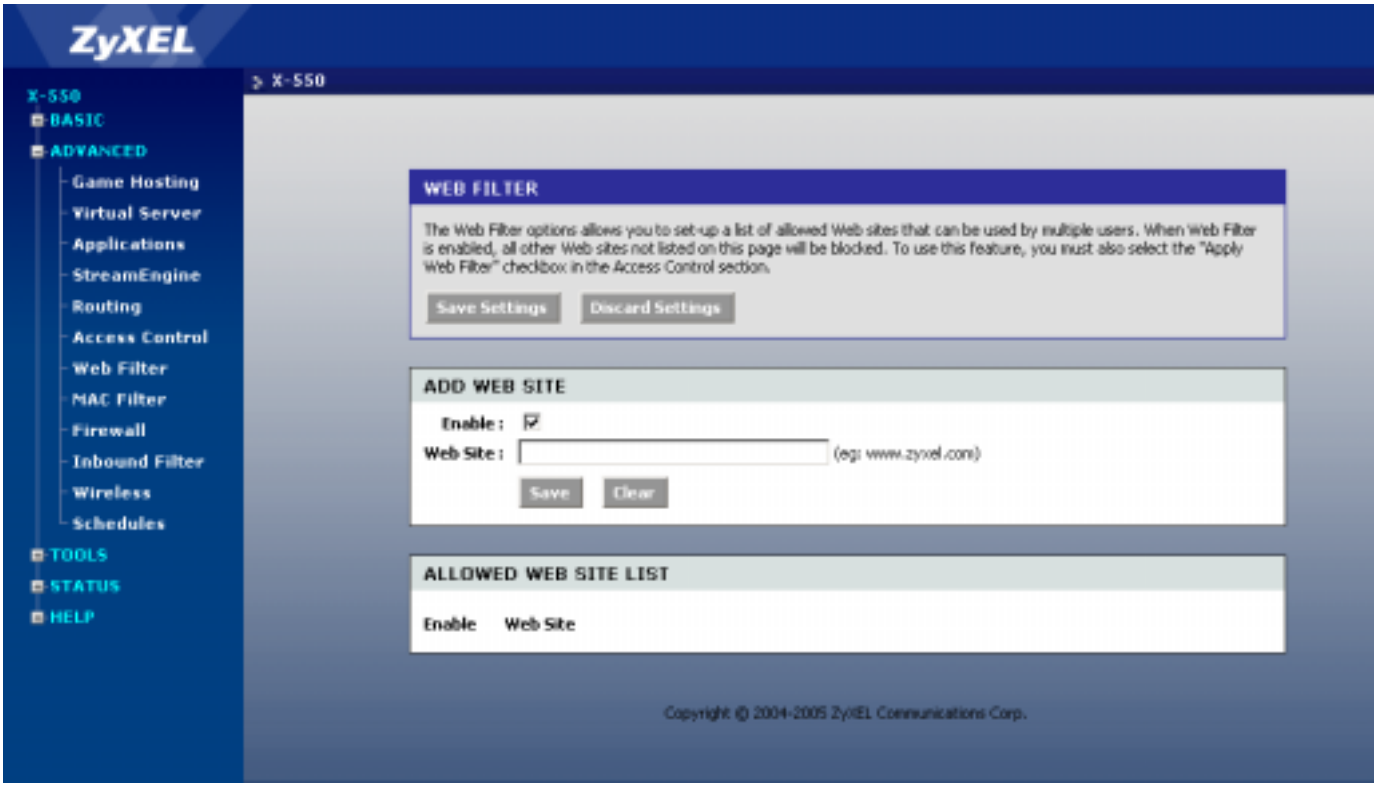


Figure 3-14 ADVANCED – Web Filter

ADD/EDIT WEB SITE

This is where you can add Web sites to the Allowed Web Site List or change entries in the Allowed Web Site List. The Allowed Web Site List is used for systems that have the **Web Filter** option enabled in **Access Control**.

Enable:

Entries in the Allowed Web Site List can be activated or deactivated with this checkbox. New entries are activated by default.

Web Site:

Enter the URL (address) of the Web Site that you want to allow; for example: **google.com**. Do not enter the **http://** preceding the URL. Enter the most inclusive domain; for example, enter **dlink.com** and access will be permitted to both **www.dlink.com** and **support.dlink.com**.

Note: Many web sites construct pages with images and content from other web sites. Access will be forbidden if you do not enable all the web sites used to construct a page. For example, to access **my.yahoo.com**, you need to enable access to **yahoo.com**, **yimg.com**, and **doubleclick.net**.

Save:

Clicking **Save** saves the new or edited Allowed Web Site in the following list. When finished updating the Allowed Web Site List, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

ALLOWED WEB SITE LIST

The section lists the currently allowed web sites. An allowed web site can be changed by clicking the Edit

icon, or deleted by clicking the Delete icon. When you click the **Edit** icon, the item is highlighted, and the "**Edit Web Site**" section is activated for editing.

3.2.8 ADVANCED - MAC Filter

The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter.

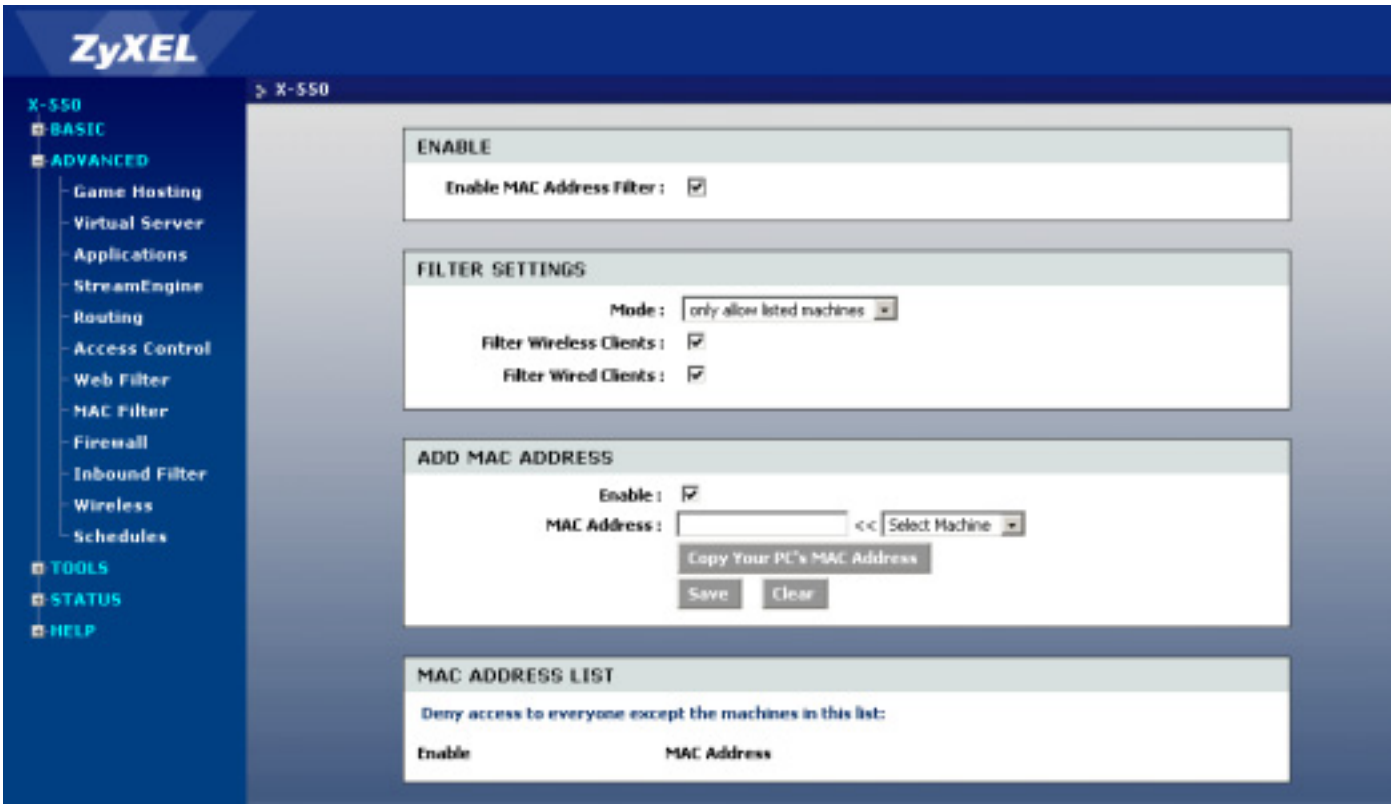


Figure 3-15 ADVANCED – MAC Filter

ENABLE MAC Address Filter:

When this is enabled, computers are granted or denied network access depending on the mode of the filter.

Configuration of this feature incorrectly can prevent any machine from accessing the network. In such a situation, you can regain access by activating the factory defaults button on the physical router itself.

FILTER SETTINGS

Mode:

- **Only Allow Listed Machines** – Only computers with MAC addresses listed in the MAC Address List are granted network access.
- **Only Deny Listed Machines** – Any computer with a MAC address listed in the MAC Address List is refused access into the network.

Filter Wireless Clients:

When this is selected, the MAC address filters will be applied to wireless network clients.

Filter Wired Clients:
When this is selected, the MAC address filters will be applied to wired network clients.

ADD MAC ADDRESS
In this section, you can add entries to the MAC Address List below, or edit existing entries.

Enable:
MAC address entries can be activated or deactivated with this checkbox.

MAC Address:
Enter the MAC address of the desired computer or connect to the router from the desired computer and click the Clone Your PC's MAC Address button.

Save:
Clicking **Save** saves the new or edited MAC Address entry in the following list. When finished updating the MAC Address List, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

MAC ADDRESS LIST
The section lists the current MAC Address filters. A MAC Address entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit MAC Address" section is activated for editing.

3.2.9 ADVANCED - Firewall

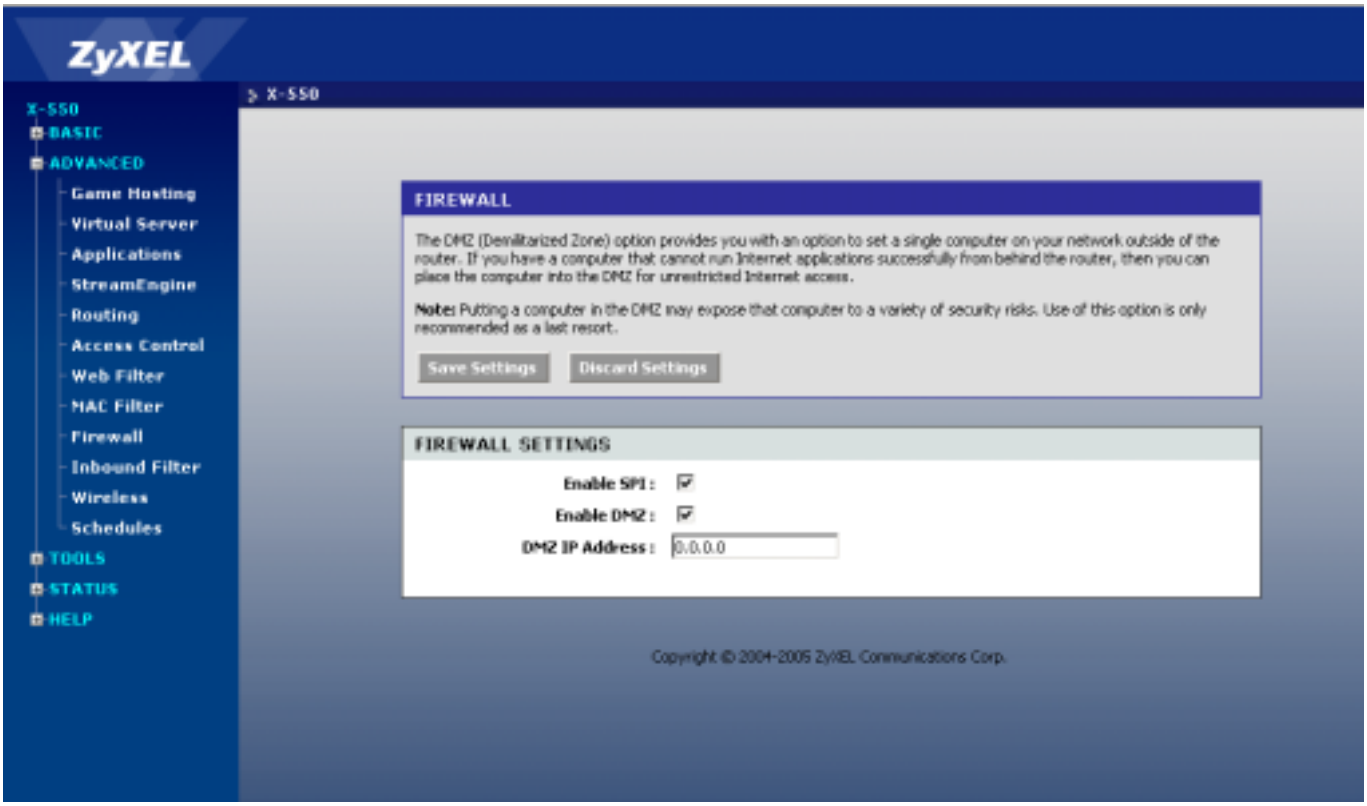

ZyXEL
X-550
BASIC
ADVANCED
Game Hosting
Virtual Server
Applications
StreamEngine
Routing
Access Control
Web Filter
MAC Filter
Firewall
Inbound Filter
Wireless
Schedules
TOOLS
STATUS
HELP
X-550
FIREWALL
The DMZ (Demilitarized Zone) option provides you with an option to set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.
Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.
Save Settings
Discard Settings
FIREWALL SETTINGS
Enable SPI :
Enable DMZ :
DMZ IP Address :
0.0.0.0
Copyright © 2004-2005 ZyXEL Communications Corp.

Figure 3-16 ADVANCED – Firewall

FIREWALL SETTINGS

Enable SPI:

SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyberattacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol. When SPI is enabled, the extra state information will be reported on the Status -> Active Sessions page.

Enable DMZ:

DMZ means "Demilitarized Zone." If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

DMZ IP Address:

Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its address Automatically using DHCP, then you may want to make a static reservation on the **BASIC -> DHCP** page so that the IP address of the DMZ machine does not change.

3.2.10 ADVANCED - Inbound Filter

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on IP Address.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Gaming, or Remote Administration features. Each filter can be used for several functions; for example a "Game Clan" filter might allow all of the members of a particular gaming group to play several different games for which gaming entries have been created. At the same time an "Admin" filter might only allows systems from your office network to access the WAN admin pages and an FTP server you use at home. If you add an IP address to a filter, the change is effected in all of the places where the filter is used.

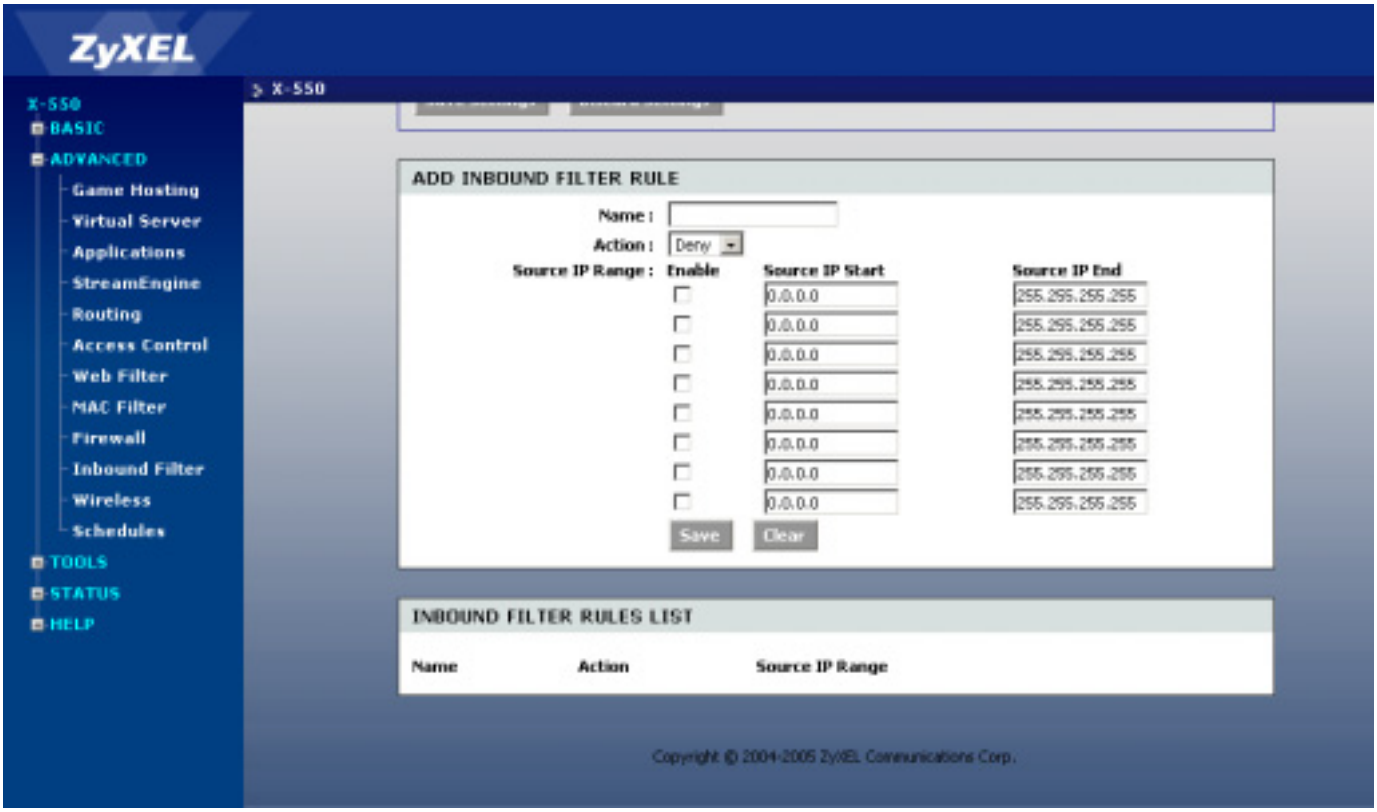


Figure 3-17 ADVANCED – Inbound Filter

ADD INBOUND FILTER RULE

Here you can add entries to the Inbound Filter Rules List below, or edit existing entries.

Name:

Enter a name for the rule that is meaningful to you.

Action:

The rule can either Allow or Deny messages.

Source IP Range:

Define the ranges of Internet addresses this rule applies to. For a single IP address, enter the same address in both the **Start** and **End** boxes. Up to eight ranges can be entered. The **Enable** checkbox allows you to turn on or off specific entries in the list of ranges.

Save:

Clicking **Save** saves the new or edited Inbound Filter Rule in the following list. When finished updating the Inbound Filter Rules List, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

INBOUND FILETER RULES LIST

The section lists the current Inbound Filter Rules. An Inbound Filter Rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Inbound Filter Rule" section is activated for editing.

In addition to the filters listed here, two predefined filters are available wherever inbound filters can be applied:

Allow:

Permit any WAN user to access the related capability.

Deny:
Prevent all WAN users from accessing the related capability. (LAN users are not affected by **Inbound Filter Rules**.)

3.2.11 ADVANCED - Wireless

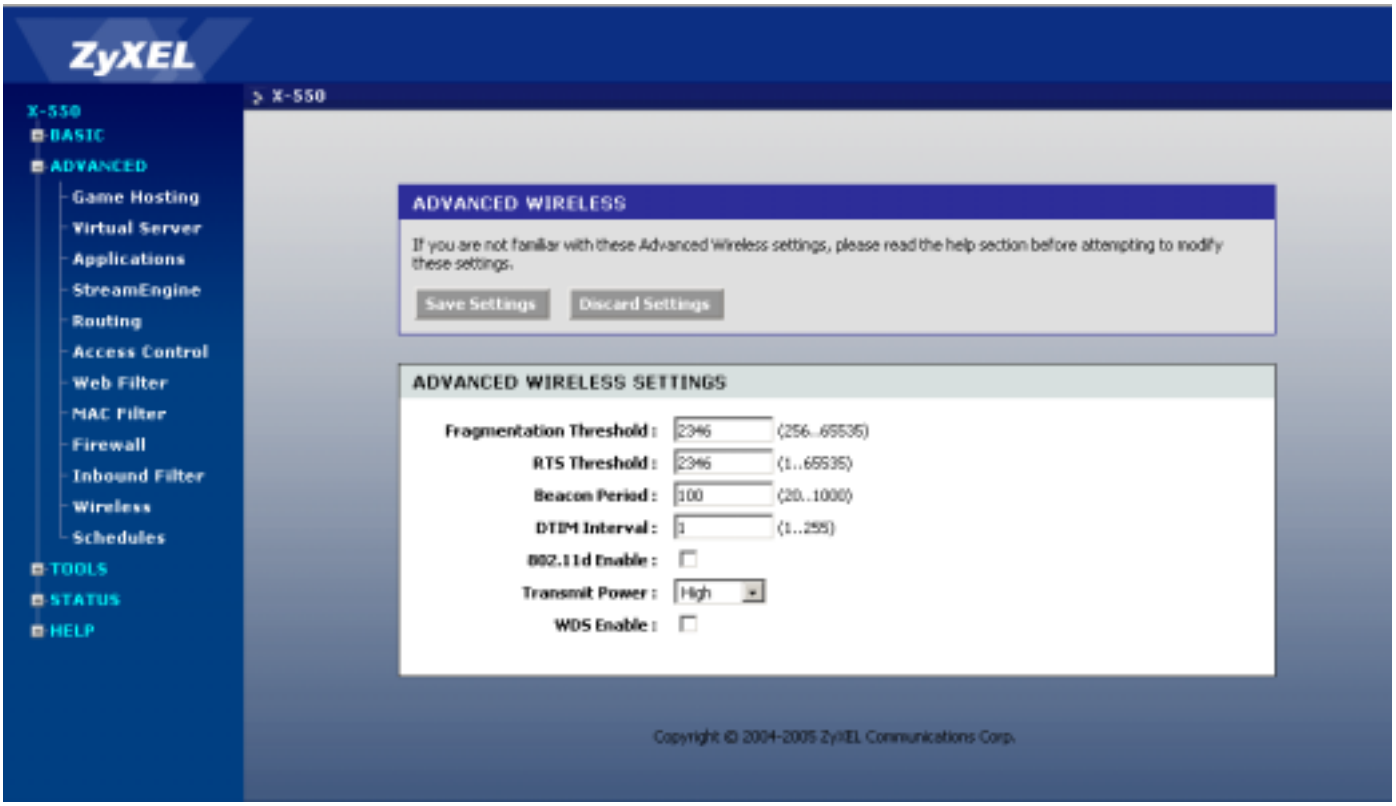


Figure 3-18 ADVANCED – Wireless

ADVANCED WIRELESS SETTINGS

Fragmentation Threshold:
This setting should remain at its default value of 2346. Setting the Fragmentation value too low may result in poor performance.

RTS Threshold:
This setting should remain at its default value of 2346. If you encounter inconsistent data flow, only minor modifications to the value are recommended.

Beacon Period:
Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.

DTIM Interval:
A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

802.11d Enable:
Checking this box enables 802.11d operation. 802.11d is a wireless specification for operation in additional

regulatory domains. This supplement to the 802.11 specifications defines the physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements to extend the operation of 802.11 WLANs to new regulatory domains (countries). The current 802.11 standard defines operation in only a few regulatory domains (countries). This supplement adds the requirements and definitions necessary to operate in markets not served by the current standard. Enable this option if you are operating in one of these "additional regulatory domains".

Transmit Power:

Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area. By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

WDS Enable:

When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links. Note that WDS is incompatible with WPA -- both features cannot be used at the same time. A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP.

3.2.12 ADVANCED - Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

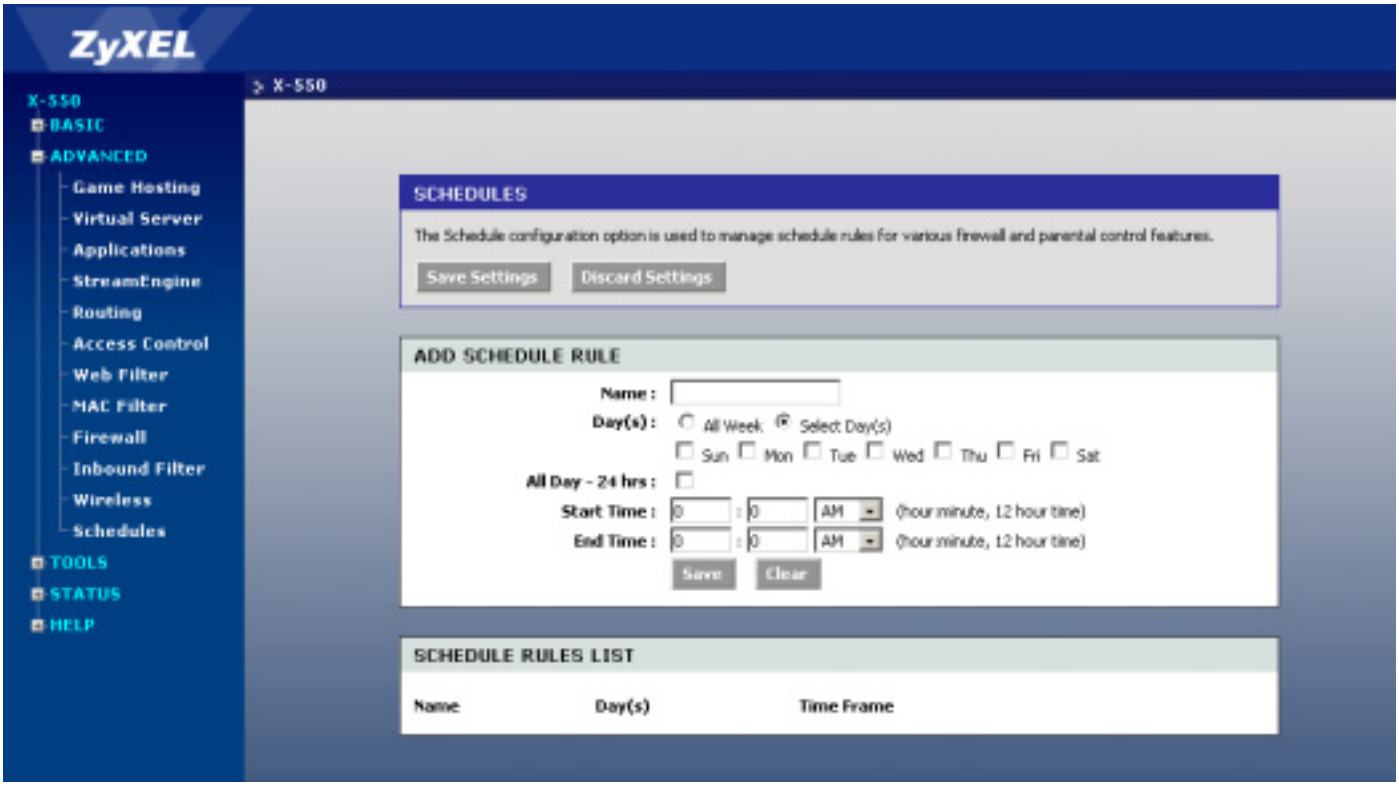


Figure 3-19 ADVANCED – Schedules

ADD SCHEDULE RULE

In this section you can add entries to the **SCHEDULE RULES LIST** below or edit existing entries.

Name:
Give the schedule a name that is meaningful to you, such as "Weekday rule".

Day(s):
Place a checkmark in the boxes for the desired days or select the All Week radio button to select all seven days of the week.

All Day - 24 hrs:
Select this option if you want this schedule in effect all day for the selected day(s).

Start Time:
If you don't use the All Day option, then you enter the time here. The start time is entered in two fields. The first box is for the hour and the second box is for the minute. Email events are triggered only by the start time.

End Time:
The end time is entered in the same format as the start time. The hour in the first box and the minutes in the second box. The end time is used for most other rules, but is not used for email events.

Save:
Clicking **Save** saves the new or edited Schedule Rule in the following list. When finished updating the Schedule Rules, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

SCHEDULE RULES LIST

The section shows the currently defined Schedule Rules. A Schedule Rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Schedule Rule" section is activated for editing.

3.3 TOOLS

The Tools tab provides the following configuration options: **Admin, Time, Syslog, Email, System, Firmware and Dynamic DNS**.

3.3.1 TOOLS - Admin

The **Admin** option is used to set a password for access to the Web-based management. By default there is no password configured. It is highly recommended that you create a password to keep your new router secure.

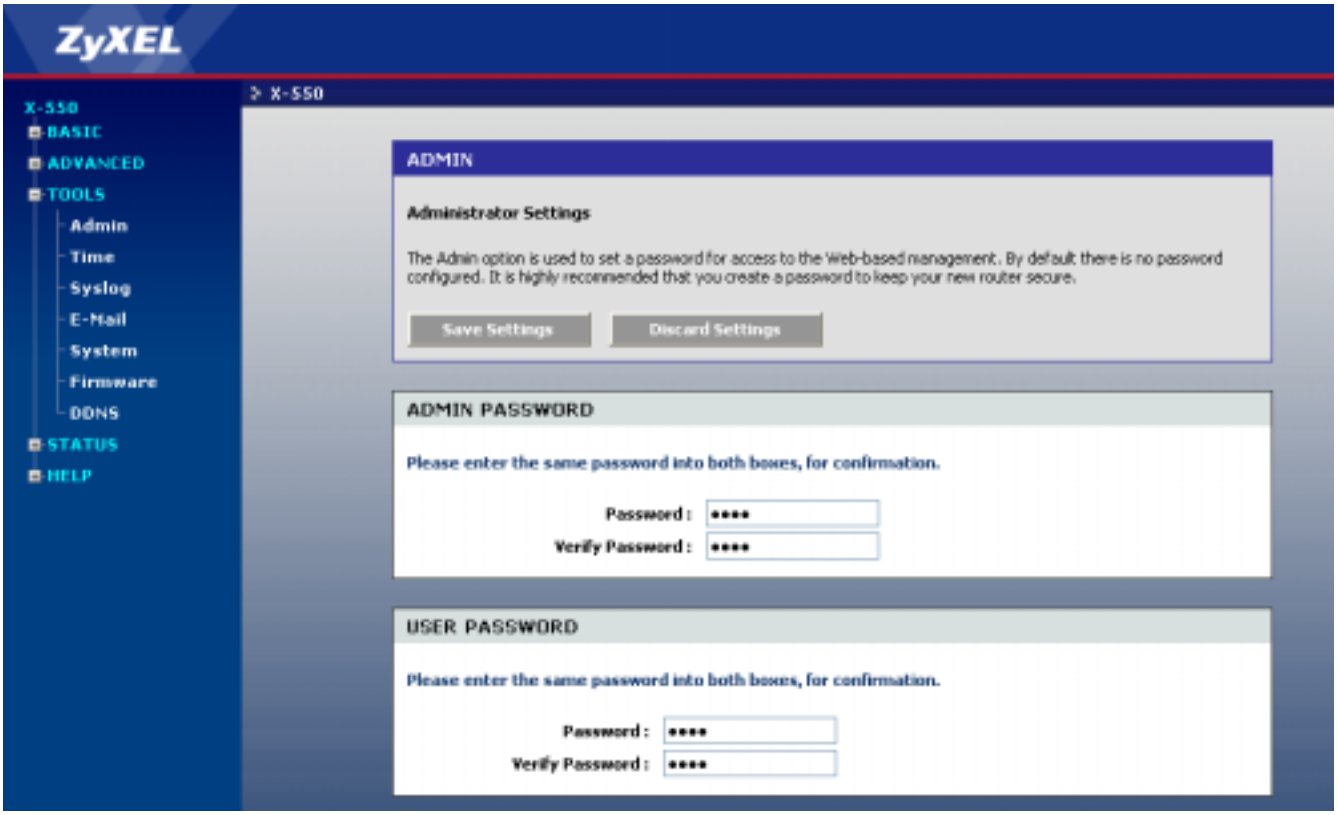


Figure 3-20 TOOLS – Admin

ADMIN PASSWORD

Enter a password for the user "**admin**", who will have full access to the Web-based management interface.

USER PASSWORD

Enter a password for the user "**user**", who will have read-only access to the Web-based management interface.

ADMISTRATION

Router Name:

The name of the router can be changed here.

Enable Remote Management:

Enabling Remote Management allows you to manage the router from anywhere on the Internet. **Disabling Remote Management** allows you to manage the router only from computers on your LAN.

Remote Admin Port:
The port that you will use to address the management interface from the Internet. For example, if you specify port 1080 here, then, to access the router from the Internet, you would use a URL of the form: **http://my.domain.com:1080/**.

Remote Admin Inbound Filter:
Select a filter that controls access as needed for this admin port. If you do not see the filter you need in the list of filters, go to the **ADVANCED -> Inbound Filter** screen and create a new filter.

Admin Idle Timeout:
The amount of time before the administration session (either remote or local) is closed when there is no activity.

UPNP

UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Wireless router. Put a check in this box to allow the router configuration to be changed by UPnP devices.

SAVE AND RESTORE CONFIGURATION

This option allows you to save the router's configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade.

Restore Configuration from File:
Use this option to load previously saved router configuration settings.

3.3.2 TOOLS - Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the router's internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight saving can also be configured to automatically adjust the time when needed.

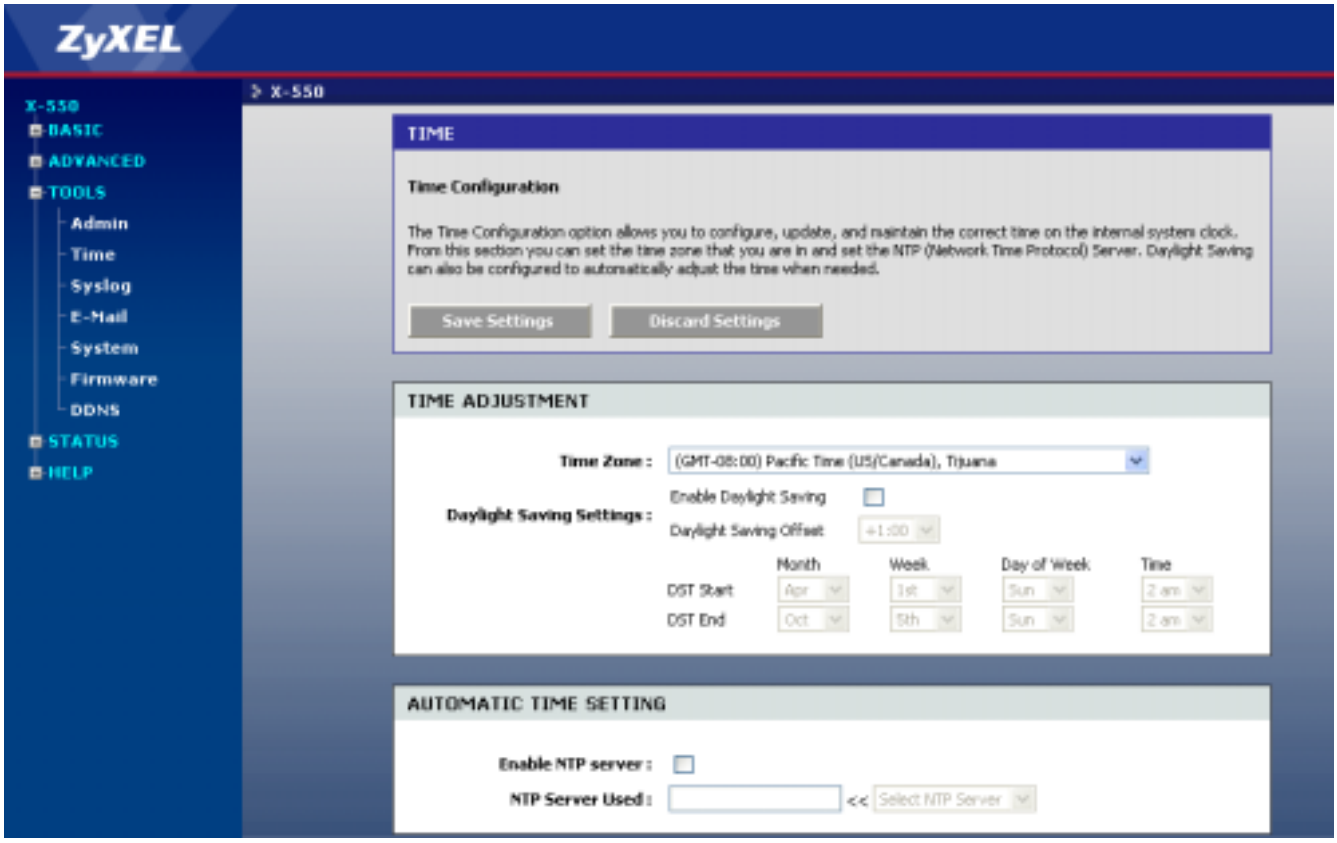


Figure 3-21 TOOLS – Time

TIME ADJUSTMENT

Time Zone:

Select your local time zone from pull down menu.

- **Daylight Saving Enable:**
  Check this option if your location observes daylight saving time.
- **Daylight Saving Offset:**
  Select the time offset, if your location observes daylight saving time.
- **DST Start and DST End:**
  Select the starting and ending times for the change to and from daylight saving time. For example, suppose for DST Start you select Month="Oct", Week="3rd", Day="Sun" and Time="2am". This is the same as saying: "Daylight saving starts on the third Sunday of October at 2:00 AM."

AUTOMATIC TIME SETTING

Enable NTP Server:

Select this option if you want the router's clock synchronized to a Network Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate.

NTP Server:
Select a Network Time Server for synchronization. You can type in the address of a time server or select one from the list. If you have trouble using one server, select another.

Set the Date and Time Manually

If you do not have the NTP Server option in effect, you can either manually set the time for your router here, or you can click the Copy Your Computer's Time Settings button to copy the time from the computer you are using. (Make sure that computer's time is set correctly.)

NOTE

If the router loses power for any reason, it cannot keep its clock running, and will not have the correct time when it is started again. To maintain correct time for schedules and logs, either you must enter the correct time after you restart the router, or you must enable the NTP Server option.

3.3.3 TOOLS - Syslog

This section allows you to archive your log files to a Syslog Server.

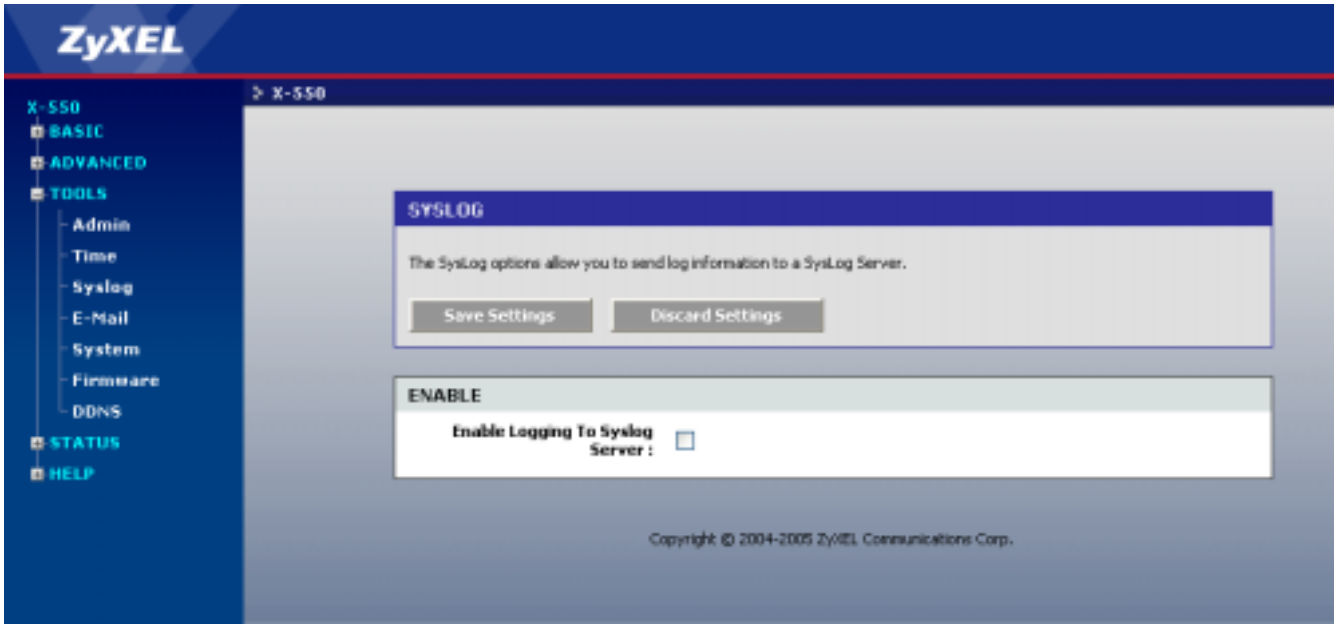


Figure 3-22 TOOLS – Syslog

Enable Logging to Syslog Server
Enable this option if you have a syslog server currently running on the LAN and wish to send log messages to it. Enabling this option causes the following parameter to be displayed.

SYSTLOG SETTINGS

Syslog Server IP Address:
Enter the LAN IP address of the Syslog Server.

3.3.4 TOOLS - Email

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.

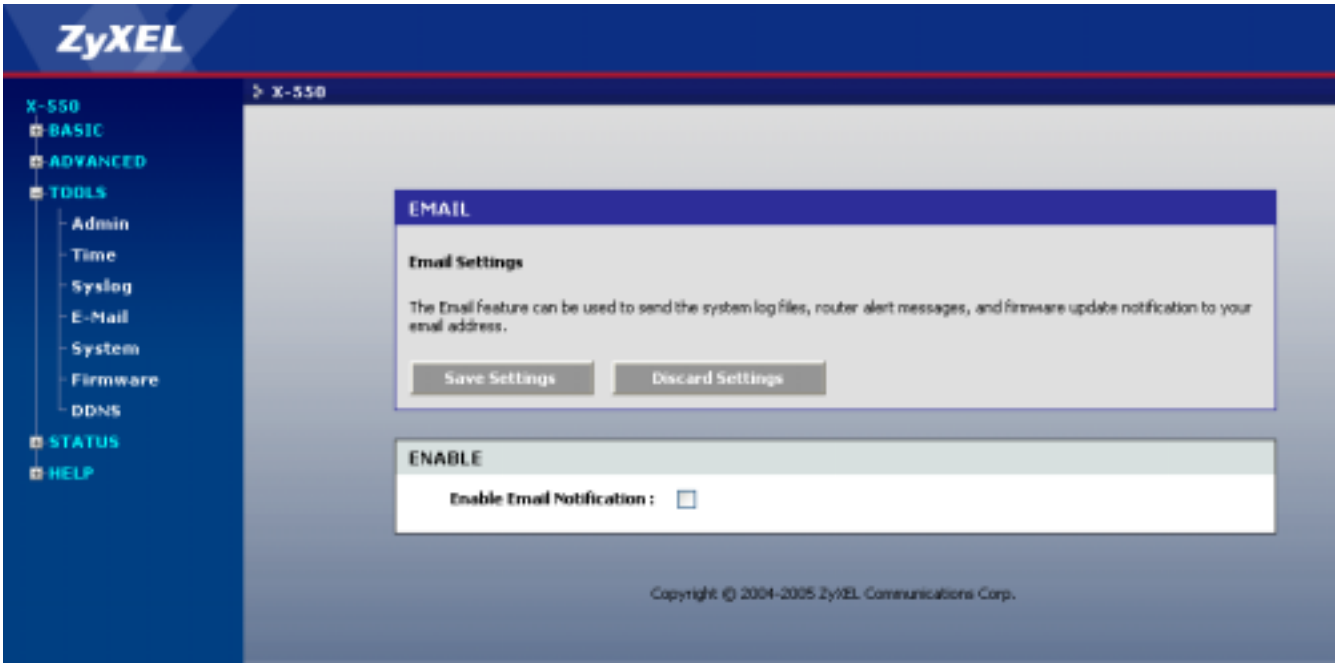


Figure 3-23 TOOLS – Email

ENABLE

Enable Email Notification:

When this option is enabled, router activity logs or firmware upgrade notifications can be emailed to a designated email address, and the following parameters are displayed.

EMAIL SETTINGS

From Email Address:

This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.

To Email Address:

Enter the email address where you want the email sent.

SMTP Server Address:

Enter the SMTP server address for sending email.

Enable Authentication:

If your SMTP server requires authentication, select this option.

Account Name:

Enter your account for sending email.

Password:

Enter the password associated with the account.

Verify Password:

Re-type the password associated with the account.

EMAIL LOG WHEN FULL OR ON SCHEDULE

On Log Full

Select this option if you want logs to be sent by email when the log is full.

On Schedule

Select this option if you want logs to be sent by email according to a schedule.

Schedule

If you selected the Schedule option, select one of the defined schedule rules. If you do not see the schedule you need in the list of schedules, go to the **TOOLS -> Schedules** screen and create a new schedule.

Email is sent at the start time defined for a schedule; the schedule end time is not used for email.

3.3.5 TOOLS - System

This section allows you to reboot the device, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

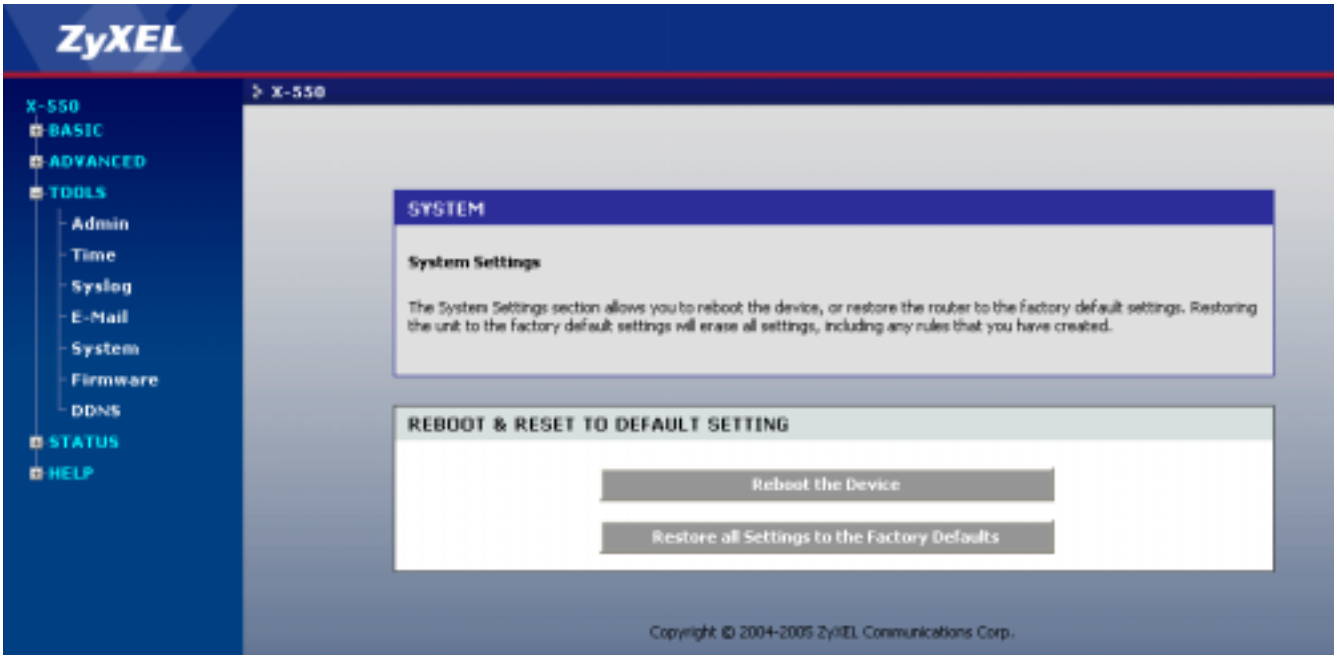


Figure 3-24 TOOLS – System

Reboot the Device

Click this button to reboot the X-550.

Restore all Settings to the Factory Defaults

This option restores all configuration settings back to the settings that were in effect at the time the router was shipped from the factory.

3.3.6 TOOLS - Firmware

The Firmware Upgrade section can be used to update your router to the latest firmware code to improve functionality and performance.

To upgrade the firmware, follow these steps:

Click the **Browse** button to locate the Wireless upgrade file on your computer.

Once you have found the file to be used, click the **Upload** button below to start the firmware upgrade process. This can take a minute or more.

Wait for the router to reboot. This can take another minute or more.

Confirm updated firmware revision on status page.

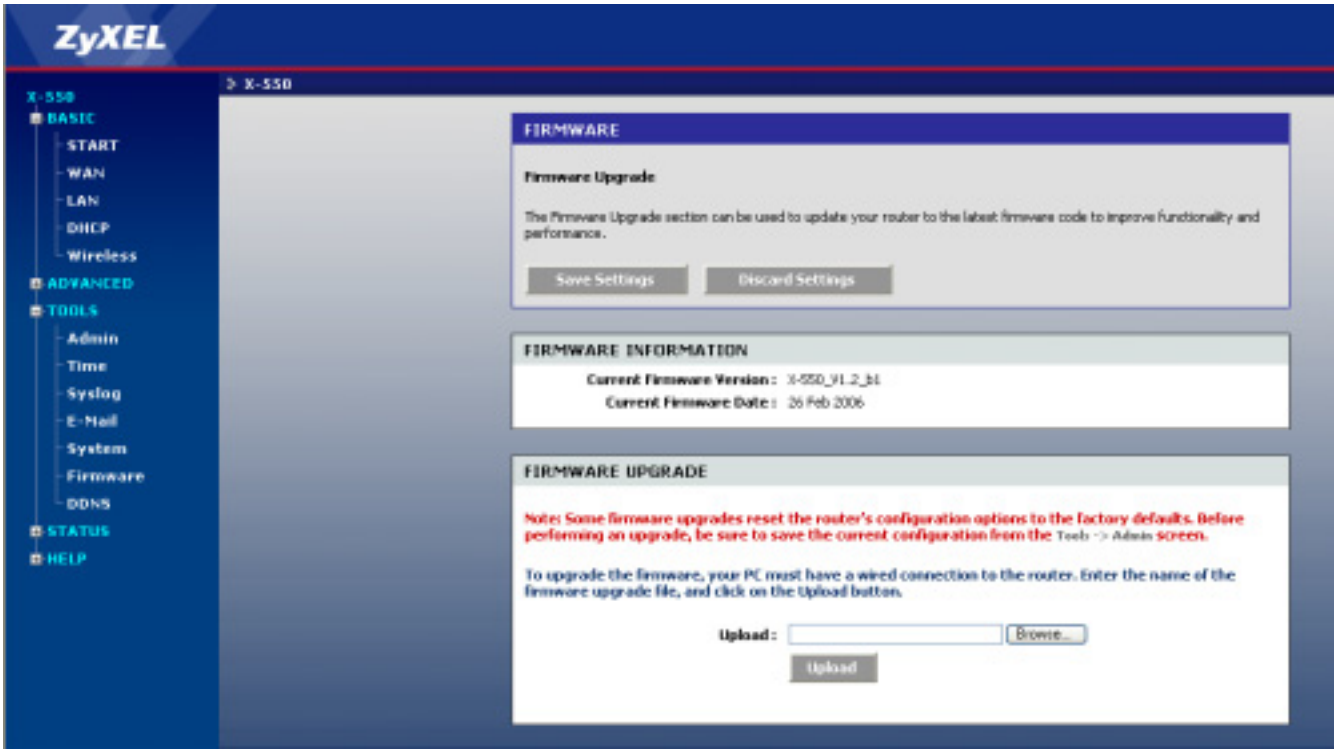


Figure 3-25 TOOLS – Firmware

FIRMWARE INFORMATION

Here are displayed the version numbers of the firmware currently installed in your router and the most recent upgrade that is available.

FIRMWARE UPGRADE

NOTE

Firmware upgrade cannot be performed from a wireless device. To perform an upgrade, ensure that you are using a PC that is connected to the router by wire.

Some firmware upgrades reset the router's configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the TOOLS -> Admin screen.

Upload

Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the router.

3.3.7 Tools - DDNS (Dynamic DNS)

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc.) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, your friends can enter your domain name to connect to your server, no matter what your IP address is.

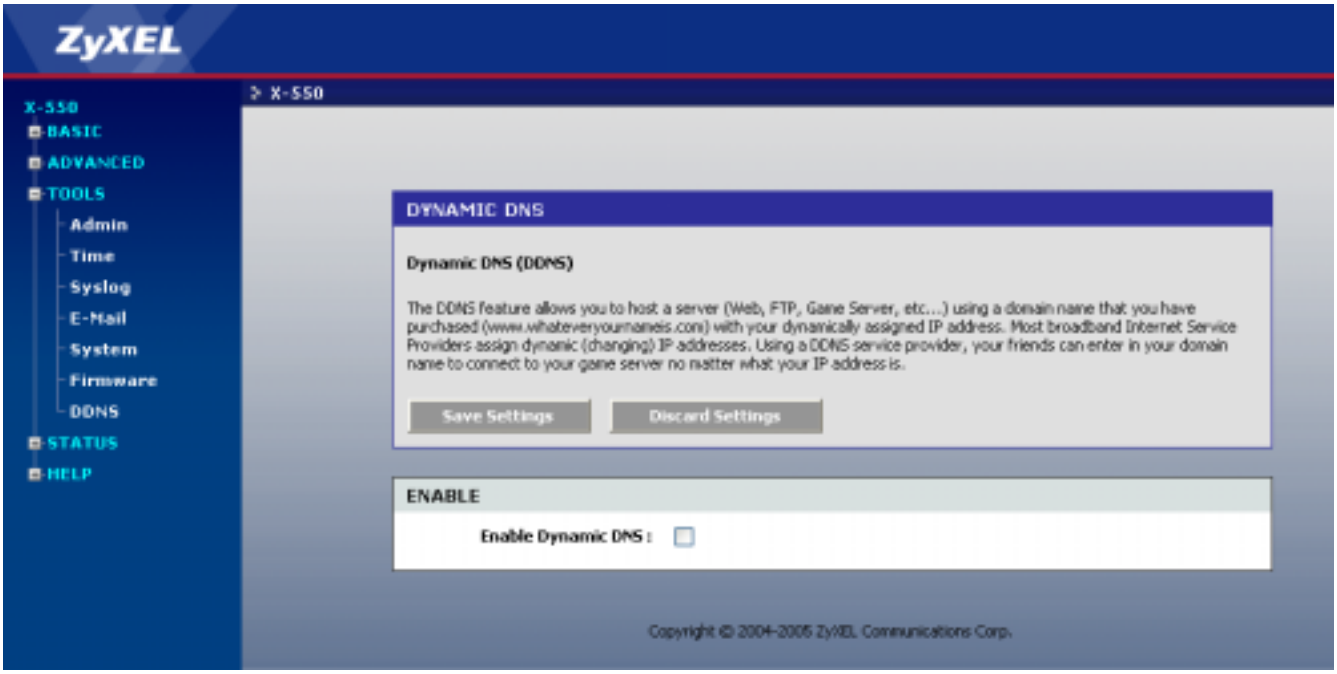

ZyXEL
X-550
BASIC
ADVANCED
TOOLS
Admin
Time
Syslog
E-Mail
System
Firmware
DDNS
STATUS
HELP
X-550
DYNAMIC DNS
Dynamic DNS (DDNS)
The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your game server no matter what your IP address is.
Save Settings
Discard Settings
ENABLE
Enable Dynamic DNS :
Copyright © 2004-2005 ZyXEL Communications Corp.

Figure 3-26 TOOLS – DDNS

Enable

Enable Dynamic DNS

Enable this option only if you have purchased your own domain name and registered with a dynamic DNS service provider. The following paramters are displayed when the option is enabled.

Server Address

Select a dynamic DNS service provider from the pull-down list.

Host Name

Enter your host name.

Username or Key

Enter the username or key provided by your service provider. If the Dynamic DNS provider supplies only a

key, enter that key in all three fields.

Password or Key

Enter the password or key provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Verify Password or Key

Re-type the password or key provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Timeout

The time between periodic updates to the Dynamic DNS, if your dynamic IP address has not changed. The timeout period is entered in hours.

After configuring the router for dynamic DNS, you can open a browser and navigate to the URL for your domain (for example http://www.mydomain.info) and the router will attempt to forward the request to port 80 on your LAN. If, however, you do this from a LAN-side computer and there is no virtual server defined for port 80, the router will return the router's configuration home page. Refer to the ADVANCED -> Virtual Server configuration page to set up a a virtual server.

3.4 STAUS

The Status tab provides the following configuration options: Device Info, Wireless, Routing, Logs, Statistics and Active Sessions.

3.4.1 STATUS - Device info

All of your Internet and network connection details are displayed on the Device Info page. The firmware version is also displayed here.

NOTE

Some browsers have limitations that make it impossible to update the WAN status display when the status changes. Some browsers require that you refresh the display to obtain updated status. Some browsers report an error condition when trying to obtain WAN status.

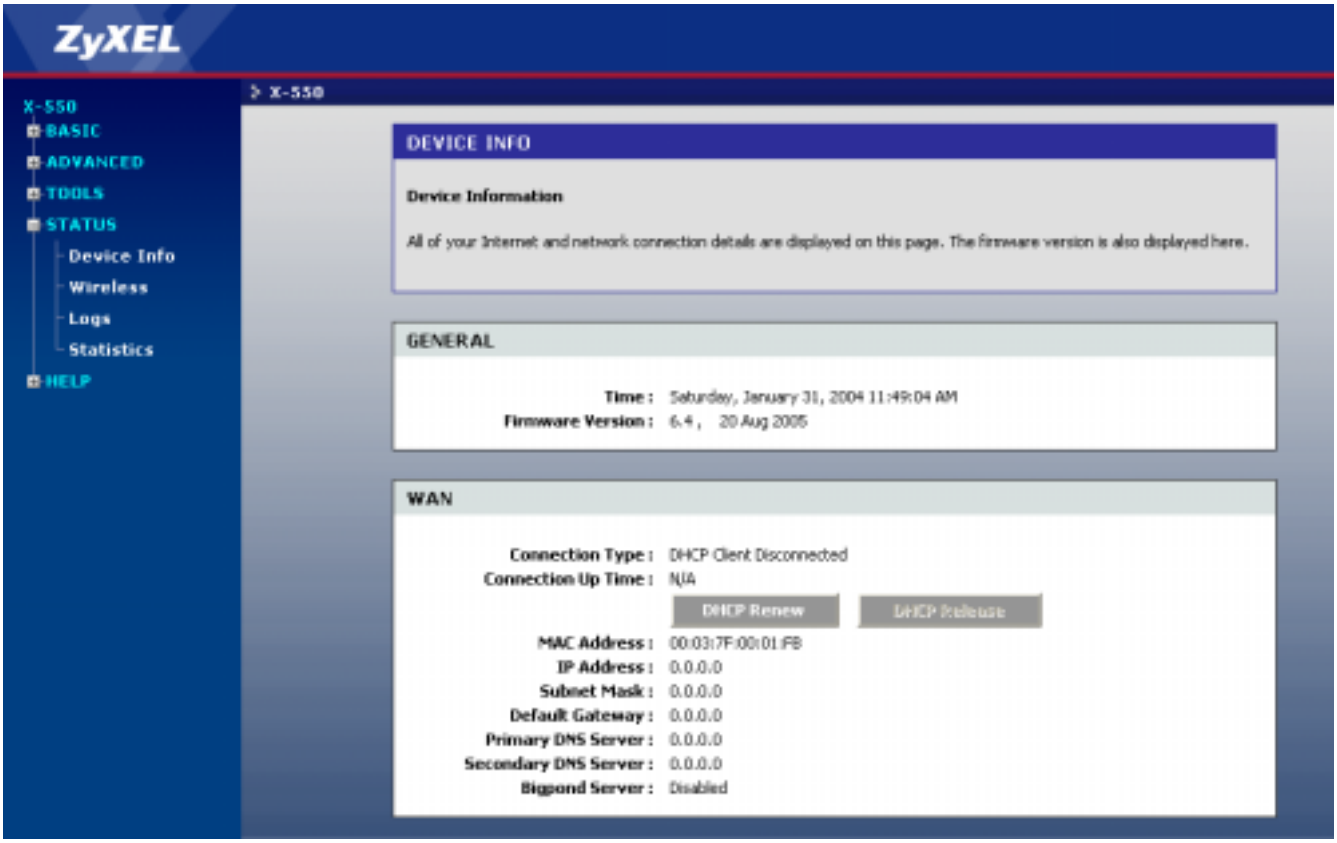


Figure 3-27 STATUS – Device Info

DHCP Connection

Clicking the **DHCP Release** button un-assigns all IP's associated with the X-550. Clicking the **DHCP Renew** button causes the router to request a new IP address from the ISP's server.

3.4.2 STATUS - Wireless

The wireless section allows you to view the wireless clients that are connected to your wireless router.

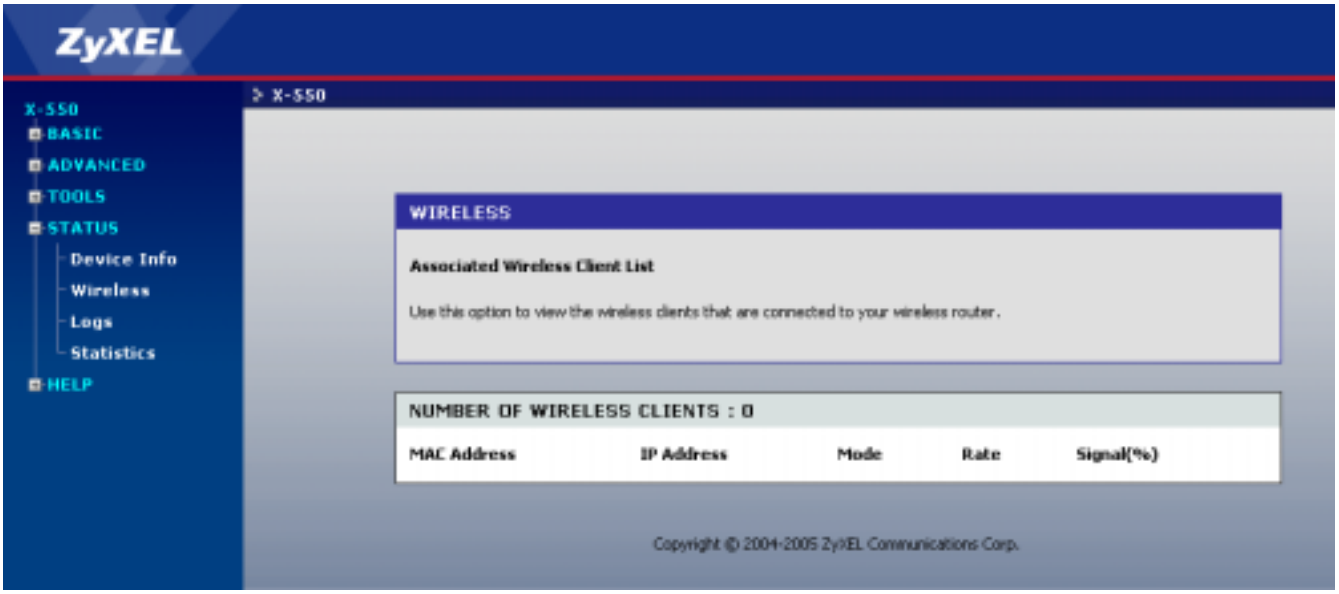


Figure 3-28 STATUS – Wireless

NUMBER OF WIRELESS CLIENTS

MAC Address

The Ethernet ID (MAC address) of the wireless client.

IP Address

The LAN-side IP address of the client.

Mode

The transmission standard being used by the client. Values are 11a, 11b, or 11g for 802.11a, 802.11b, or 802.11g respectively.

Rate

The actual transmission rate of the client in megabits per second.

Signal

This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the router and the wireless device.

3.4.3 STATUS - Logs

The router automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

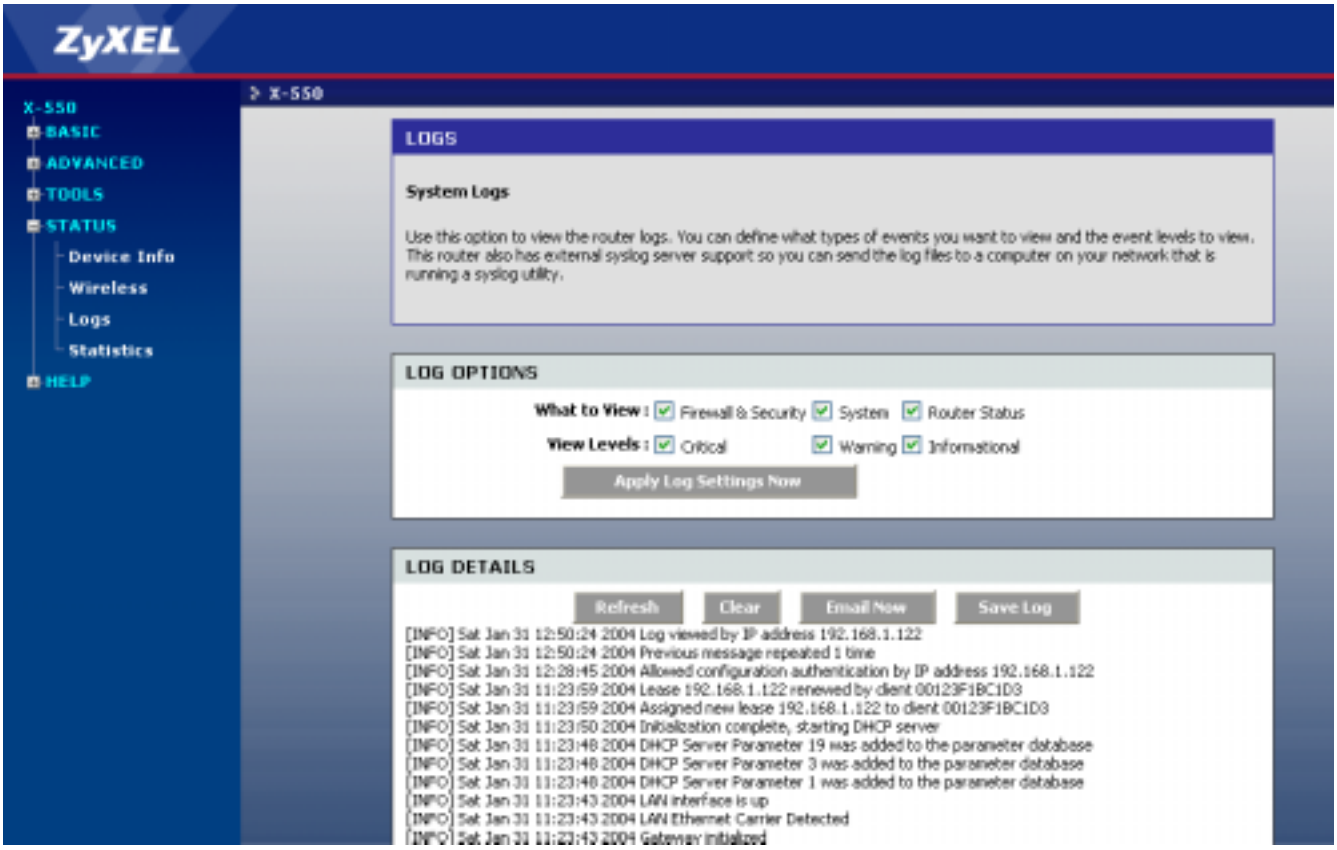

ZyXEL
X-550
BASIC
ADVANCED
TOOLS
STATUS
Device Info
Wireless
Logs
Statistics
HELP
> X-550
LOGS
System Logs
Use this option to view the router logs. You can define what types of events you want to view and the event levels to view. This router also has external syslog server support so you can send the log files to a computer on your network that is running a syslog utility.
LOG OPTIONS
What to View : Firewall & Security System Router Status
View Levels : Critical Warning Informational
Apply Log Settings Now
LOG DETAILS
Refresh
Clear
Email Now
Save Log
[INFO] Sat Jan 31 12:50:24 2004 Log viewed by IP address 192.168.1.122
[INFO] Sat Jan 31 12:50:24 2004 Previous message repeated 1 time
[INFO] Sat Jan 31 12:28:45 2004 Allowed configuration authentication by IP address 192.168.1.122
[INFO] Sat Jan 31 11:23:59 2004 Lease 192.168.1.122 renewed by client 00123F1BC1D3
[INFO] Sat Jan 31 11:23:59 2004 Assigned new lease 192.168.1.122 to client 00123F1BC1D3
[INFO] Sat Jan 31 11:23:50 2004 Initialization complete, starting DHCP server
[INFO] Sat Jan 31 11:23:48 2004 DHCP Server Parameter 19 was added to the parameter database
[INFO] Sat Jan 31 11:23:48 2004 DHCP Server Parameter 3 was added to the parameter database
[INFO] Sat Jan 31 11:23:48 2004 DHCP Server Parameter 1 was added to the parameter database
[INFO] Sat Jan 31 11:23:43 2004 LAN interface is up
[INFO] Sat Jan 31 11:23:43 2004 LAN Ethernet Carrier Detected
[INFO] Sat Jan 31 11:23:43 2004 Gateway initialized

Figure 3-29 STATUS – Logs

What to View

Select the kinds of events that you want to view.

- Firewall and Security
- System
- Router Status

View Levels

Select the level of events that you want to view.

- Critical
- Warning
- Informational

Apply Log Settings Now

Click this button after changing Log Options to make them effective and permanent.

Refresh

Clicking this button refreshes the display of log entries. There may be new events since the last time you accessed the log.

Clear

Clicking this button erases all log entries.

Email Now

If you provided email information with the **TOOLS -> Email** screen, clicking the **Email Now** button sends the router log to the configured email address.

Save Log

Select this option to save the router log to a file on you computer.

3.4.4 STATUS - Statistics

The Statistics page displays all of the LAN, WAN, and Wireless packet transmit and receive statistics.

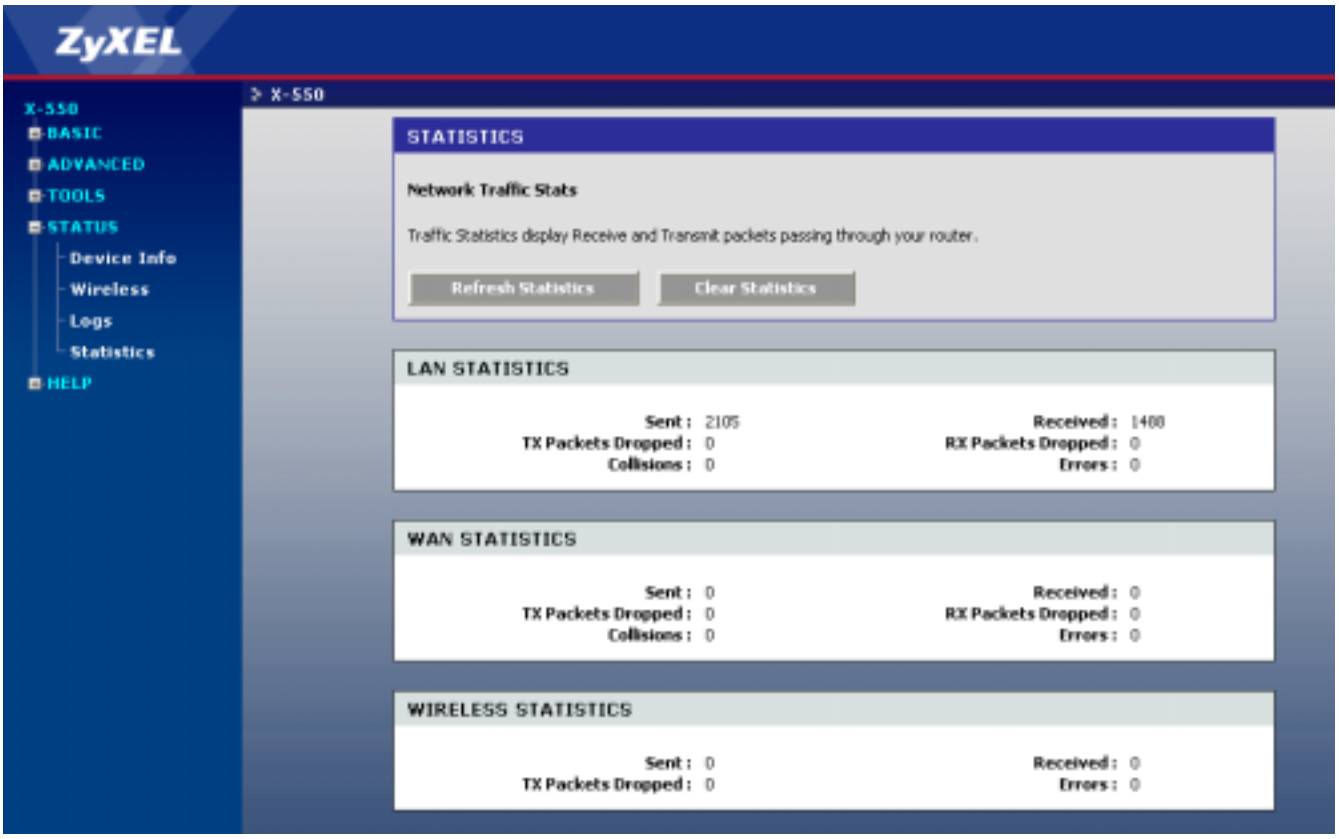


Figure 3-30 STATUS – Statistics

STATISTICS

Sent

The number of packets sent from the router.

Received

The number of packets received by the router.

TX Packets Dropped

The # of packets that were dropped transmitting, due to errors, collisions, or router resource limitations.

RX Packets Dropped

The # of packets that were dropped receiving, due to errors, collisions, or router resource limitations.

Collisions

The number of packets that were dropped due to Ethernet collisions which are caused when two or more devices attempt to use an Ethernet circuit at the same time

Errors

The number of transmission failures that cause loss of a packet. A noisy radio-frequency environment can cause a high error rate on the wireless LAN.

Glossary

A

Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

Access Point

AP. Device that allows wireless clients to connect to it and access the network

ActiveX

A Microsoft specification for the interaction of software components.

Ad-hoc network

Peer-to-Peer network between wireless clients

Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

ADSL

Asymmetric Digital Subscriber Line

Advanced Encryption Standard

AES. Government encryption standard

Alphanumeric

Characters A-Z and 0-9

Antenna

Used to transmit and receive RF signals.

AppleTalk

A set of Local Area Network protocols developed by Apple for their computer systems

AppleTalk Address Resolution Protocol

AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer

7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

Automatic Private IP Addressing

APIPA. An IP address that that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

B

Backward Compatible

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth

The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Basic Input/Output System

BIOS. A program that the processor of a computer uses to startup the system once it is turned on

Baud

Data transmission speed

Beacon

A data frame by which one of the stations in a Wi-Fi network periodically broadcasts network control data to other wireless stations.

Bit rate

The amount of bits that pass in given amount of time

Bit/sec

Bits per second

BOOTP

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Bottleneck

A time during processes when something causes the process to slowdown or stop all together

Broadband

A wide band of frequencies available for transmitting data

Broadcast

Transmitting data in all directions at once

Browser

A program that allows you to access resources on the web and provides them to you graphically

C

Cable modem

A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

CardBus

A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

CAT 5

Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client

A program or user that requests data from a server

Collision

When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie

Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

D

Data

Information that has been translated into binary so that it can be processed or moved to another device

Data Encryption Standard

Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

Data-Link layer

The second layer of the OSI model. Controls the movement of data on the physical link of a network

Database

Organizes information so that it can be managed updated, as well as easily accessed by users or applications.

DB-25

A 25 ping male connector for attaching External modems or RS-232 serial devices

DB-9

A 9 pin connector for RS-232 connections

dBd

Decibels related to dipole antenna

dBi

Decibels relative to isotropic radiator

dBm

Decibels relative to one milliwatt

Decrypt

To unscramble an encrypted message back into plain text

Default

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

Demilitarized zone

DMZ: A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP

Dynamic Host Configuration Protocol: Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them

Digital certificate:

An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum

DSSS: Modulation technique used by 802.11b wireless devices

DMZ

"Demilitarized Zone". A computer that logically sits in a "no-mans land" between the LAN and the WAN. The DMZ computer trades some of the protection of the router's security mechanisms for the convenience of being directly addressable from the Internet.

DNS

Domain Name System: Translates Domain Names to IP addresses

Domain name

A name that is associated with an IP address

Download

To send a request from one computer to another and have the file transmitted back to the requesting computer

DSL

Digital Subscriber Line. High bandwidth Internet connection over telephone lines

Duplex

Sending and Receiving data transmissions at the sane time

Dynamic DNS service

Dynamic DNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always by linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports Dynamic DNS, whenever the IP address changes

Dynamic IP address

IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

E

EAP

Extensible Authentication Protocol

Email

Electronic Mail is a computer-stored message that is transmitted over the Internet

Encryption

Converting data into cyphertext so that it cannot be easily read

Ethernet

The most widely used technology for Local Area Networks.

F

Fiber optic

A way of sending data through light impulses over glass or plastic wire or fiber

File server

A computer on a network that stores data so that the other computers on the network can all access it

File sharing

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights

Firewall

A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware

Programming that is inserted into a hardware device that tells it how to function

Fragmentation

Breaking up data into smaller pieces to make it easier to store

FTP

File Transfer Protocol. Easiest way to transfer files between computers on the Internet

Full-duplex

Sending and Receiving data at the same time

G

Gain

The amount an amplifier boosts the wireless signal

Gateway

A device that connects your network to another, like the internet

Gbps

Gigabits per second

Gigabit Ethernet

Transmission technology that provides a data rate of 1 billion bits per second

GUI

Graphical user interface

H

H.323

A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices

Half-duplex

Data cannot be transmitted and received at the same time

Hashing

Transforming a string of characters into a shorter string with a predefined length

Hexadecimal

Characters 0-9 and A-F

Hop

The action of data packets being transmitted from one router to another

Host

Computer on a network

HTTP

Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS

HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub

A networking device that connects multiple devices together

I

ICMP

Internet Control Message Protocol

IEEE

Institute of Electrical and Electronics Engineers

IGMP

Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

IIS

Internet Information Server is a WEB server and FTP server provided by Microsoft

IKE

Internet Key Exchange is used to ensure security for VPN connections

Infrastructure

In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet

A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer

A World Wide Web browser created and provided by Microsoft

Internet Protocol

The method of transferring data from one computer to another on the Internet

Internet Protocol Security

IPsec provides security at the packet processing layer of network communication

Internet Service Provider

An ISP provides access to the Internet to individuals or companies

Intranet

A private network

Intrusion Detection

A type of security that scans a network to detect attacks coming from inside and outside of the network

IP

Internet Protocol

IP address

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec

Internet Protocol Security

IPX

Internetwork Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

ISP

Internet Service Provider

J

Java

A programming language used to create programs and applets for web pages

K

Kbps

Kilobits per second

Kbyte

Kilobyte

L

LAN

Local Area Network

Latency

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED

Light Emitting Diode

Legacy

Older devices or technology

Local Area Network

A group of computers in a building that usually access files from a server

LPR/LPD

"Line Printer Requestor"/"Line Printer Daemon". A TCP/IP protocol for transmitting streams of printer data.

L2TP

Layer 2 Tunneling Protocol

M

MAC address

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

Mbps

Megabits per second

MDI

Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX

Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

MIB

Management Information Base is a set of objects that can be managed by using SNMP

Modem

A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE

Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU

Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

Multicast

Sending data from one device to many devices on a network

N

NAT

Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI

NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS

Network Basic Input/Output System

Netmask

Determines what portion of an IP address designates the Network and which part designates the Host

Network Interface Card

A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network Layer

The third layer of the OSI model which handles the routing of traffic on a network

Network Time Protocol

Used to synchronize the time of all the computers in a network

NIC

Network Interface Card

NTP

Network Time Protocol

O

OFDM

Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

OSI

Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF

Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

P

Password

A sequence of characters that is used to authenticate requests to resources on a network

Personal Area Network

The interconnection of networking devices within a range of 10 meters

Physical layer

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

Ping

A utility program that verifies that a given Internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

PoE

Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

POP3

Post Office Protocol 3 is used for receiving email

Port

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet channel) but can have multiple ports (logical channels) each identified by a number.

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble

Used to synchronize communication timing between devices on a network

Q

QoS

Quality of Service

R

RADIUS

Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Reboot

To restart a computer and reload it's operating software or firmware from nonvolatile storage.

Rendezvous

Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater

Retransmits the signal of an Access Point in order to extend it's coverage

RIP

Routing Information Protocol is used to synchronize the routing table of all the routers on a network

RJ-11

The most commonly used connection method for telephones

RJ-45

The most commonly used connection method for Ethernet

RS-232C

The interface for serial communication between computers and other related devices

RSA

Algorithm used for encryption and authentication

S

Server

A computer on a network that provides services and resources to other computers on the network

Session key

An encryption and decryption key that is generated for every communication session between two computers

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

Simple Mail Transfer Protocol

Used for sending and receiving email

Simple Network Management Protocol

Governs the management and monitoring of network devices

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SOHO

Small Office/Home Office

SPI

Stateful Packet Inspection

SSH

Secure Shell is a command line interface that allows for secure connections to remote computers

SSID

Service Set Identifier is a name for a wireless network

Stateful inspection

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass though the firewall

Subnet mask

Determines what portion of an IP address designates the Network and which part designates the Host

Syslog

System Logger -- a distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

T

TCP

Transmission Control Protocol

TCP/IP

Transmission Control Protocol/Internet Protocol

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TFTP

Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput

The amount of data that can be transferred in a given time period

Traceroute

A utility displays the routes between you computer and specific destination

U

UDP

User Datagram Protocol

Unicast

Communication between a single sender and receiver

Universal Plug and Play

A standard that allows network devices to discover each other and configure themselves to be a part of the network

Upgrade

To install a more recent version of a software or firmware product

Upload

To send a request from one computer to another and have a file transmitted from the requesting computer to the other

UPnP

Universal Plug and Play

URL

Uniform Resource Locator is a unique address for files accessible on the Internet

USB

Universal Serial Bus

UTP

Unshielded Twisted Pair

V

Virtual Private Network

VPN: A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN

Virtual LAN

Voice over IP

Sending voice information over the Internet as opposed to the PSTN

VoIP

Voice over IP

W

Wake on LAN

Allows you to power up a computer though it's Network Interface Card

WAN

Wide Area Network

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with all of the information on the World Wide Web

WEP

Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wi-Fi

Wireless Fidelity

Wi-Fi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption

Wide Area Network

The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network

Wireless ISP

A company that provides a broadband Internet connection over a wireless connection

Wireless LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP

Wireless Internet Service Provider

WLAN

Wireless Local Area Network

WPA

Wi-Fi Protected Access. A Wi-Fi security enhancement that provides improved data encryption, relative to WEP.

X

xDSL

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Y

Yagi antenna

A directional antenna used to concentrate wireless signals on a specific location

Z

#

1

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).